□ 元宇宙规制

规范元宇宙：可能性、难题与基本思路……丁　玮　於兴中　3
元宇宙的法律规制……丁道勤　20
元宇宙金融规制理论……邓建鹏　35
元宇宙对著作权法的挑战与回应……张金平　54
NFT 交易模式下的著作权保护及平台责任……王江桥　70
元宇宙的法律难题…[印尼] 萨法里·卡西亚安托　[德] 穆斯塔法·基林茨　著
郑志峰　罗有成　译　81

□ 数字经济治理

社会信用建构
——基于大数据征信治理的探究……黎四奇　93
论流量传导行为对数字经济平台市场力量的影响……杨　东　王　睿　113
论算法个性化定价的解构与规制
——祛魅大数据杀熟……雷　希　124
公共决策算法的程序规范
——以立法性算法为例……刘佳明　141
论数字时代的美术作品原件
——基于展览权的视角……李　强　154
算法解释在民法中的体系定位与类型区分……胡巧莉　刘征峰　168
破产程序中数据权益之保护
——以信义义务为视角……程　威　184
互联网不正当竞争类型化条款司法适用的反思与纠正……黄　军　201

限制数据抓取行为的违法性认定
——以美国干扰侵权理论为视角……高建成 217
全球数据治理的 DEPA 路径和中国的选择 ……靳思远 323
虚拟货币的国际监管：以反洗钱为起点走出自发秩序……吴 云 朱 玮 247
自由贸易协定金融信息传送规则构建……马 光 卜小翠 266

□ 个人信息保护

信息主体同意的适用边界……李群涛 高富平 280
论信息主体的知情同意及其实现……常宇豪 295
个人信息保护“目的限制原则”的反思与重构
——以《个人信息保护法》第 6 条为中心……朱荣荣 311
数字防疫中个人信息治理的“链”“法”协同机制研究……胡元聪 龚家锋 325
“国家在场”视角下个人信息保护的实践检视与路径探索……王 娅 340
被遗忘权本土化的路径选择与规范重塑
——以《个人信息保护法》第 4 条为中心……王义坤 刘金祥 355
论个人信息侵权中的损害……朱晓峰 夏 爽 369
个人信息私法救济中的“损害赔偿”困境与应对路径……赵贝贝 385
论超大型平台独立机构的功能构造
——以《个人信息保护法》第 58 条为中心 …… 韩 阳 397

财经法学 No. 5，2022
pp. 3 - 19

规范元宇宙：可能性、难题与基本思路

丁　玮　於兴中*

内容提要：虽然当下热议的“元宇宙”是一个缺乏明确定义的概念，但是“数字化生存”的愿景和想象启示了人类进入数字化社会形态的各种可能性。元宇宙本身不是一种方法，也不是一种技术，而是一个集人的游戏（玩）、好赌及趋利性三种主要特性于一身的商业概念。人的这三种特性构成了元宇宙的核心。元宇宙发展的方向取决于人类自身的选择和建构，虚拟世界与现实世界在法律关系上具有同一性、关联性和相似性，虚拟世界的规范秩序建构依赖于现实世界的法律概念、原则和制度。未来元宇宙是以法律规则为核心的组织化、规则化和秩序化的秩序建构过程。法律规制和政府监管对虚拟世界来说是必需的，谁来管控元宇宙是重要的议题，在宪法层面对元宇宙的私权力进行有效规制，对于塑造更美好的未来具有结构性的基础作用。

关键词：元宇宙　再中心化　虚拟世界

一、引言

进入信息社会后，互联网、移动通信、云计算、大数据和人工智能等技术发展的速度远超人类文明的任何阶段。在数字化和智能化的大背景下，人类的生存空间逐渐从物理空间拓展到虚拟空间，“数字化生存”的愿景和想象启示了人类进入数字化社会形态的各种可能性，元宇宙（metaverse）概念的横空出世看似颠覆了人类的想象，又好似技术发展和进步的水到渠成。这是一个人人皆知的术语，但仍然是一个缺乏明确定义的概念。这是一个吸引了最大的科技公司——苹果、Meta、微软——最聪明的头脑的想法，但没有人真正知道它将会是什么。

* 丁玮，哈尔滨工程大学人文社会科学学院副教授；於兴中，澳门大学法学院讲座教授、西安交通大学法学院海外讲座教授。

本文为2021年度国家社会科学基金项目“数字社会私权力宪法规制研究”（21BFX043）、中央高校基本科研业务费专项资金资助项目“数字法学视域下公民数字素养培育研究”（HEU3072022WK1313）的阶段性成果。

元宇宙的概念对不同的人来说显然意味着非常不同的东西。现存的是一系列雏形的数字空间，如脸书（Facebook）的 Horizon、Epic Games 的 Fortnite、罗布乐思（Roblox）的游戏和游戏创作数字空间，以及基于区块链的数字世界 Decentraland。所有这些都有明确的边界、不同的规则和目标以及不同的增长速度。

尽管如此，比较清楚的是，元宇宙正在到来。它将把今天的互联网与虚拟现实（VR）、增强现实（AR）和区块链技术相结合。它将是一个人们相互交流的地方，在那里购买和销售商品和服务，在那里围绕教育、文化、娱乐和信仰形成社区，而个人数据、财产和隐私的传统边界将会被弃之不顾。在某些方面，它将与我们已经知道的数字世界相似，而在其他方面，它将完全不同。

元宇宙是否能够真正成为引领未来数字技术发展的方向，成为人类文明进化历史中的奇点，取决于人类自身的选择和建构。在当下关于元宇宙的热议和评论中，基本问题仍然如赫拉利在《人类简史》中的灵魂拷问："我们人类究竟想要什么？"在元宇宙中智人历史是飞跃还是终幕？元宇宙已在哲学、传播学、文学、社会学、经济学等众多人文社会科学领域引起较大关注。目前，最重要的是人们开始初步探索元宇宙的监管问题。尽管人们很清楚监管一个尚未成型的对象并非易事，但这并不妨碍对元宇宙监管问题进行探索。元宇宙是否有必要监管？元宇宙有哪些可能的风险？法律如何面对未来元宇宙的秩序建构？本文试图对这些问题进行探讨。

二、元宇宙概念的理想与现实

目前尚没有一个关于元宇宙本身的科学定义。一般的定义往往是对数字技术所驱动和连接的信息空间的一种概括性描述。〔1〕元宇宙是一个连接使用者所有生活方面的线上、3D 和虚拟空间概念。这个概念将引导多个平台连接在一起，就像今天的互联网一样，通过一个单一的浏览器进入多个网页。本质上，元宇宙的概念可以理解为一个由相互连接的，并且可由公共界面进入的，融合 2D 和 3D 要素的深度互联网虚拟世界组成的大规模基础设施。因此，没有单一的实体可以被称为元宇宙，元宇宙是通过数字化和 3D 网络工具的多个实体的共同合作进入我们的环境，成为我们生活的一部分。〔2〕

（一）文学叙事中的想象

元宇宙或许被认为是互联网发展的终局，但其并不是互联网发展的产物。众所周知，元宇宙的概念由尼尔·斯蒂芬森在 1992 年出版的恶托邦（Distopia）科幻小说《雪崩》（Snow Crash）发展而来。〔3〕这一概念的流行夸大了小说《雪崩》在赛博朋克科幻史上的地位。美国学者吉尔·莱波雷（Jill Lepore）认为元宇宙"马斯克主义"是一种奢侈的资本主义形式，其来源正是批判资本主义的科幻故事。〔4〕元宇宙并不是人们向往的地方，而是逃避丑恶现实的地方。

〔1〕 参见段伟文：《探寻元宇宙治理的价值锚点——基于技术与伦理关系视角的考察》，载《国家治理》2022 年第 2 期。

〔2〕 See Kevin W. Allen, *Metaverse*, Copyright by Kevin W. Allen, 2022, p. 7.

〔3〕 参见〔美〕尼尔·斯蒂芬森：《雪崩》，郭泽译，四川科学技术出版社 2017 年版。

〔4〕 参见〔美〕吉尔·莱波雷：《元宇宙、马斯克主义？科技富翁们的外星资本主义》，载 https://www.sohu.com/a/500614847_115479，最后访问时间：2022 年 7 月 1 日。

西方科幻文学的基调是科技悲观主义。人们发现科技进步总是带来种种问题，人的生存处境似乎比工业革命前更加艰难，第一部科幻小说《弗兰肯斯坦》讲述的就是技术伦理悲剧。20 世纪 60、70 年代的科技悲观主义与流行的朋克文化结合形成的赛博朋克文学范式，具有向权威和旧秩序抗争的进步意义。但是，赛博朋克追求感官享受，缺乏对科技走向反人类、技术资本垄断等问题更深层次的思考，使得这一文学形式像一股风一样很快就刮过去了。《雪崩》开启了“后赛博朋克”阶段，小说没有赛博朋克故事中常见的压抑的世界秩序和悲壮的反抗运动，只剩下荒诞的元宇宙喜剧。换言之，这里只有赛博，没有朋克。〔5〕在面对技术利维坦的巨大压迫和垄断下，人们无法形成有效反抗，转而投身其所批判的科技愿景中，成为臣服于感官享乐的数字奴隶，这反映了文学对现实批判力的减弱甚至丧失。《雪崩》文学叙事中的元宇宙是一种隐喻，它隐喻了当前对元宇宙概念的热炒，资本和大众对科技寡头的拥抱，以及未来的技术、社会与人类的关系。

（二）游戏中的现实

《雪崩》之后最先将元宇宙想象应用于虚拟世界的就是虚拟游戏。1995 年的虚拟世界 Active World，2003 年的开放式游戏《第二人生》（ Second Life）都受到了斯蒂芬森小说的影响。在虚拟游戏发展分期中，第一阶段是 20 世纪 70 年代文本互动游戏，《龙与地下城》（Dungeons and Dragons1974）和《洞穴探险》（ Colossal Cave Adventure1975），被视为元宇宙的史前叙述；第二阶段为 20 世纪 90 年代 3D 图像和开放式社交的虚拟世界，包括 1994 年的多人社交游戏 Web World 和 1995 年的内容创作虚拟世界 Active World；第三阶段为 21 世纪以后大规模多人在线数字游戏和开放式游戏，以《第二人生》和《机器砖块》（ Roblox）为代表。〔6〕

有学者认为，虚拟游戏是虚拟美学的一大领域。它采用虚拟现实技术构建高度仿真的虚拟存在世界，具有技术、动作、意境、内涵等方面的审美特征，可以产生虚实相生的独特审美效应。〔7〕例如，我国《古剑奇谭》是虚拟游戏艺术的一个代表，这种艺术形式充分运用了虚拟现实技术，通过角色设计、场景设计和光影效果设计，构建出一个高度仿真的虚拟世界，产生独特的审美效应，让玩家在其中获得感官的“沉浸”，补充和延展了现实世界的不足，从而有效调节人们在现实世界中的失衡心态，也折射出深厚的美学思想。〔8〕笔者认为，与其说虚拟游戏属于虚拟美学的范畴，莫不如说虚拟游戏使虚拟幻想以更逼近梦境的样态带给人避世和快感。元宇宙创生出一种“叙事的永远现实态”，它更巧妙地掩盖了市场垄断、利润剥夺和价值操控的存在，人们不必用“规训或惩罚”的条令来管理自己，元宇宙轻松实现人们的“平等感”“自由感”，取代社会平等和政治自由本身。快感已经可以成为财产。我们为了快感而在游戏中储币，更会“氪金”。元宇宙叙事正是完全鼓励这种快感或者说享乐实体化的形式，让文学艺术和社会生活越来越趋于快感化。只要给身体制造相应的感知设备、提供快感场景，人就会被机器制造出来的快感

〔5〕 参见陈韬：《面对“元宇宙”，科幻文艺怎样保持批判力》，载《中国文艺评论》2022 年第 2 期。
〔6〕 参见胡泳、刘纯懿：《“元宇宙社会”：话语之外的内在潜能与变革影响》，载《南京社会科学》2022 年第 1 期。
〔7〕 参见夏洁：《虚拟游戏的审美特征及价值》，载《美与时代（上）》2016 年第 12 期。
〔8〕 参见夏洁：《论虚拟游戏的审美特征——以〈古剑奇谭〉为例》，载《参花（下）》2014 年第 10 期。

直接支配。〔9〕虚拟游戏的发展受到元宇宙文学想象的影响，而虚拟游戏的进一步发展反过来又加深和拓展了未来元宇宙的构想，也就是说，文学和游戏在勾画元宇宙概念和未来愿景中起到引领作用。

（三）商业上的资本运作

“元宇宙”并非“新概念”，2021 年之所以能被冠以元宇宙元年，皆因资本的入场。2021 年是人们开始认真谈论元宇宙的一年，这可能并非偶然。在新冠疫情大流行期间，许多事情，从社交到购物到工作，都因为需求而数字化了，以至于有时感觉我们似乎已经进入了元宇宙的一半。事实上，我们还没有进入甚至还没有接近元宇宙。随着脸书（Facebook）调整商业布局，资本市场随之起舞，元宇宙成为业界和投资者的热门概念。2021 年 3 月，元宇宙概念第一股罗布乐思（Roblox）在美国纽约证券交易所正式上市，招股书里面直接提到了元宇宙；2021 年 5 月，脸书宣布将在 5 年内转型成一家元宇宙公司，并于 10 月 28 日更名为“Meta”；2021 年 8 月，字节跳动斥巨资收购 VR 创业公司 Pico.；2021 年 11 月 23 日，在虚拟世界平台 Decentraland 里，一块数字土地被卖出 243 万美元。

2022 年以来，元宇宙已经超越了斯蒂芬森 1992 年首创这个词汇时所赋予的沉浸式 3D 虚拟世界的内涵，拓展至物理世界中的物体、行动者、界面以及构建起虚拟环境并与之交互的网络等。〔10〕虽然元宇宙在过去只是一个文学中的科幻概念，但现在它看起来会在未来成为现实。元宇宙将利用增强现实技术，使每个用户都能够控制一个角色或者化身，参加混合现实会议，在虚拟办公室使用 Oculus VR 完成工作，用以区块链为基础的游戏来放松，然后管理数字加密货币钱包和金融，所有这一切都发生在元宇宙中。

支持者认为，除了支持游戏、社交媒体，元宇宙将连接经济、数字身份、去中心化治理以及其他应用。即使在今天，用户创造结合有价值的所有权和金钱将帮助发展独特的元宇宙。所有这些能力将赋予区块链在未来技术中巨大的潜在权力。而批评者则认为，科技渐进式的进步才是常态。当前在技术突破、新的需求、主体功能等方面没有任何新的东西，元宇宙更像是一个概念炒作，而且它也符合概念炒作的基本特点，目前业界和学界都没有将虚拟现实、虚拟游戏、静态三维建模、数字孪生、传感器与元宇宙相区别，而是混同使用。〔11〕

通过以上三个方面对元宇宙由来的梳理可以看出，元宇宙与当前互联网的区别主要是被称为“共同在场”（co-presence）的维度，即在同一个数字空间感受他人在场的能力。它不同于当前技术和平台应用的 2D 平面数字空间，是一种具有三维深度的数字传感器空间。已经问世的虚拟游戏世界已经具有一些元宇宙的因素，这些应用接近元宇宙，但还不是元宇宙。现在，元宇宙并不存在。在元宇宙概念的背后是已然渗透到人类社会生活方方面面的数字资本主义，人们生活在数字资本主义所构造的域之中，遵循着被定义的规则，自由时间被占用和填充，元宇宙似乎并没有

〔9〕参见周志强：《元宇宙、叙事革命与某物的创生》，载《探索与争鸣》2021 年第 12 期。

〔10〕参见前引〔1〕，段伟文文。

〔11〕参见贾韬：《“元宇宙热的冷思考”笔谈（上）》之《概念先行后的一地鸡毛：元宇宙会是例外?》，载《科学经济社会》2022 年第 1 期。

· 6 ·

带来什么不同。〔12〕未来，元宇宙能否给人类社会带来全方位的变革，并塑造出一个全新的社会形态，除了交给时间没有人能说得清楚。但是，对可能世界的可能问题展开前瞻性研究仍然是值得的。

三、元宇宙的实质

从2021年下半年开始，元宇宙逐渐进入媒体世界，成为一个使用率较高的词汇。然而，频繁使用该词的，也就是为元宇宙鼓与呼的，基本上是游戏公司和投资公司的代理人。2022年7月18日，《时代》杂志发表了一篇题为《元宇宙将重塑我们的生活，让我们确保它变得更好》的文章。作者马修·鲍尔是知名的元宇宙支持者，也是控股公司Epyllion的CEO，风险投资公司Makers Fund的风险合伙人。他在文中指出，直到现在人们还没有一个比较清晰的元宇宙的概念，而元宇宙的产品也尚未问世，关于它的计划也没有落地，尽管对元宇宙的投资已经超过1200亿美元。〔13〕

不过，重要的是鲍尔使用了定冠词来形容元宇宙（The Metaverse），这意味着元宇宙是一个独一无二的存在。事实上，苹果公司、微软、Meta、罗布乐思等公司都在开发自己的元宇宙。这就是说，很可能有若干个而不是一个独一无二的元宇宙。与此相关的是，有一种说法认为元宇宙是和我们的现实世界平行的另一个世界。〔14〕与我们的世界平行的，会是一个什么样的世界？如果说是网络世界，即虚拟/拟真世界是和现实世界平行的世界，那倒也说得通。然而，元宇宙仅仅是网络世界中的若干个场域，或者是游乐场，或者是赌场，或者是办公场所。它不是一个特定的世界，而是一个特定的世界中的若干个组成部分。所谓元宇宙是我们的平行世界的说法是站不住脚的。

众所周知，任何事物都有它内在的规定性，不管我们如何称呼它，本质、基本特点或者基本规定性，这样一种内核是存在的。尽管我们今天已经不太强调本质主义，但我们可以用其他的词汇来形容这种情况。从元宇宙概念的起源来看，它不是一个技术概念，不是一个科学概念，不是一个哲学概念，不是一个历史概念，也不是一个文学概念。如前所述，它是一个从科幻小说里产生出来，被游戏公司试图变为现实的商业性概念。职是之故，元宇宙并不具有研究的学术价值。

元宇宙本身不是一种方法，也不是一种技术，它只是试图将各种主要用于娱乐的尖端技术融合到一起，创造一个环境、一个场域或者一个空间的愿景。它将是一个虚拟现实空间，用户可以

〔12〕参见高奇琦、梁兴洲：《幻境与虚无：对元宇宙现象的批判性反思》，载《学术界》2022年第2期。

〔13〕See Mathew Ball, The Metaverse Will Reshape Our Lives. Let's Make Sure It's for the Better, Time, July 18, 2022, available at https://time.com/6197849/metaverse-future-matthew-ball/, last visited on Jul. 25, 2022.

〔14〕参见《元宇宙已经来了，或许就是传说中的平行世界》，载https://www.kepuchina.cn/Article/articleInfo?business_type=100&classify=0&ar_id=83853，最后访问时间：2022年7月26日；小七有书：《你相信吗？在现实世界之外，真的存在另一个世界》，载https://baijiahao.baidu.com/s?id=1738050177203007894&wfr=spider&for=pc，最后访问时间：2022年7月26日；柳浪闻莺眺西子：《“元宇宙”到底是什么？一个跟现实世界平行运行的人造空间》，载http://www.360doc.com/content/20/0813/07/71135856_1004666238.shtml，最后访问时间：2022年7月26日。

· 7 ·

在其中与计算机生成的环境和其他用户进行互动。元宇宙很可能成为一类虚拟空间的代称，而不是特指某一个大的虚拟空间。也就是说它不是跟我们的宇宙或现实世界平行的另外一个世界，而是若干个大玩场，其中有两路玩家：一路是在里面玩的小朋友，一路是在外面赚钱的商家。

游戏公司罗布乐思在招股书里提到，元宇宙有八个重要特征，即身份、朋友（社交）、沉浸感、随时随地、低延迟、内容的多元化、经济、安全。〔15〕扎克伯格认为，元宇宙就是一组相互连接的数字空间，能让你在其中做一些物理世界中无法做到的事情，而重要的是，它将以社会存在为特征，无论你碰巧在世界哪个角落，你都能感觉到与另外一个人在一起。他强调，他们不像别人那样只是讨论工具，讨论人和物，他们想要做的是联系人与人，要以人为中心。〔16〕然而，按照常人的理解，既然要以人为中心，我们本来就在现实世界中，为什么要到虚拟世界中生活？扎克伯格的元宇宙也要通过虚拟现实的头盔或者类似设备的链接，以化身进入，计划使用加密货币，支持 NFT，然后有临场感、沉浸感、即时感等。

在一定意义上，元宇宙实际上就是一种幻境，把有些人偶尔做的梦变成可以重复的梦。戴上头盔和手套，即可进入一个梦幻的自由世界，可以随意追求现实中无法实现的目标。一旦取下头盔，即刻回到现实，梦境荡然无存。而且，做梦是需要花钱的。

它很可能是网上的迪士尼，迪士尼的增强版。当然，这是比较客气的说法。《金融时报》的一位作者说，元宇宙实际上是拉斯维加斯的最新化身。〔17〕这种说法虽然夸张，但也指出了一些问题。比如，现在在元宇宙中热炒的 NFT，多少有赌博的意味，而且玩和赌往往交织在一起。

但这并不意味着元宇宙本身没有生命力。相反，元宇宙的生命力会非常强大。不过，这种强大并不是因为它的科学性或逻辑性，而是因为它集成了人的三种主要特性，即游戏（玩耍）、好赌和趋利。这三种特性构成了元宇宙的核心结构。这是一个无法打破的铁三角关系，极少有人能够抗拒它的诱惑。因此，不管元宇宙的概念有多不清楚，有多虚幻，人们还是要追捧，资本还是会进入。

正是因为元宇宙的核心是玩、赌与资本的紧密结合，所以元宇宙一旦发展，其势头猛不可挡。各行各业都会进军元宇宙。万物皆可元宇宙。元宇宙是不是伪命题，谜底尚未揭开。但是，某些产业已经将其作为一种创新的营销手端。目前，涉及元宇宙概念的上市公司比比皆是，虽然大多数公司还没有任何与元宇宙有关的产品。〔18〕

四、规范元宇宙的必要性

为了成为可行的生活和商业场所，元宇宙需要现实世界的控制，以保护用户免受滥用、欺诈

〔15〕 See veled, What is the meta universe?, Matters, available at https://matters.news/@veledaseohwv/211982-what-is-the-meta-universe-bafyreidy6kzrt2qka6ewqgvrx6f2fg6pyimkpwabsjkruwtdjltl7gwwqe, last visited on Aug. 29, 2022.

〔16〕 See Mark Zuckerberg, Founder's Letter, 2021, Meta, available at https://about.fb.com/news/2021/10/founders-letter/, last visited on Aug. 29, 2022.

〔17〕 See Izabella Kaminska, The metaverse is just the latest incarnation of Las Vegas, Financial Times, available at https://www.ft.com/content/739235bc-c418-4895-a426-3bd245ec6a00, last visited on Aug. 29, 2022.

〔18〕 参见於兴中、沈岿：《“元宇宙”：玩家的利益与知识分子的责任》，载“中国法律评论”微信公众号，2021 年 12 月 20 日。

和损失。然而，有效监管需要时间，也很难在全球范围内实施。重要的是，首先要认识到对元宇宙监管的必要性。元宇宙不再是科幻，必须要考虑它可能带来的威胁，无论是对个人消费者还是对企业。如果元宇宙真正可行，监管机构和这些虚拟空间的设计者现在就应该努力确保其用户的安全。元宇宙存在着风险。现实世界和虚拟世界的交融预示着一种大的社会转变，存在对现有法律制度、财产制度以及消费者隐私的挑战，因此我们不得不慎重对待。

（一）元宇宙中的风险

元宇宙中的交易充满风险。首先，我们在虚拟世界中交换的不是传统意义上的货币，它们要么是加密货币，要么是《堡垒之夜》（V-Bucks）中的游戏内货币。可能有账户或钱包来存储这些资产，但没有政府支持的保护措施来防止损失或欺诈。其次，我们在元宇宙中买卖东西的价值不如现实世界中那么明显。一个不可替换（非同质）的代币（NFT）或一块虚拟房地产可能看起来有价值，但情况并不一定如此，也没有退款权或其他的消费者保护。再次，还有更多的传统风险，如欺诈。我们还不知道网络犯罪分子可能利用元宇宙的所有方式。但比较清楚的是，无论是通过黑客攻击还是身份盗窃，虚拟世界并不能避免现实世界已经存在的安全问题。更重要的是，我们在心理上也面临重大风险。如果元宇宙看起来和感觉起来像现实世界一样，但却不受刑法的约束，并且有更极端的体验，那么就会有围绕创伤和负面心理健康影响的重大风险。

（二）前所未有的社会转型

元宇宙意味着从以第三人称观看的平面媒体到以第一人称体验的沉浸式媒体的巨大社会转型。用户的角色，从外部的观察者变成了内部的参与者。换句话说，现实世界和虚拟世界如何衔接、融合仍然是未知数。社会生活的方方面面都可能受到影响，但如何影响、影响多大，目前难以判断。自从互联网诞生以来，网络空间已经发生了很多变化，我们甚至可以预测未来的生活将受到影响。然而，未来可能比想象中离我们更近。元宇宙是一个三维的虚拟领域，用户可以利用先进的人机交互接口（HCI）技术与虚拟环境互动。元宇宙提供了一种虚拟现实的体验，让人们沉浸在不同类型或形式的现实中。它是物理现实和数字现实的混合体。我们正经历着生活方式的转变，如虚拟环境、增强现实应用程序、社交网络和虚拟世界。新技术将我们最疯狂的科学幻想变为现实，而这将改变我们的生活。一些人认为这是互联网的未来。我们将习惯于被限制在家里，与世隔绝，在巨大的虚拟景观中进行全球旅行。〔19〕另一方面，这种变化实际上意味着平台供应商，即管理这些大型平台的实体，将拥有更多的控制权、影响力和对人们生活的了解。消费者处于被动地位。这更充分证明了监管的必要性。

（三）对现行法律的挑战

元宇宙中的活动，包括经济活动，明显地对现行法律制度构成了挑战。

首先，虚拟身份的主体地位。元宇宙所构想的虚拟世界，是与现实世界平行和交互融合的数字化生存空间。相较于目前的平面 2D 互联网空间，其进化和发展表现在，人类可以其化身在元宇宙中生活、生产、交易、娱乐。如果元宇宙从梦想走进现实，就会形成两个世界，每个人都有自己的化身。由此引发的法律问题是，化身是否具有独立的法律主体资格，能否具有权利能力和

〔19〕 See K. Bavanaa, Privacy in the Metaverse, 2 *Jus Corpus Law Journal* 1 (2022).

· 9 ·

行为能力，进而为其行为承担相应的法律责任。如果不具有独立的法律主体资格，而是由其“主人”承担责任，那么接下来会产生新的法律问题，比如如何界定元宇宙中化身的行为的性质。例如，当用户通过化身进行互动时，发生争吵该如何处理？如果发生在现实世界的人之间，很可能会违反侵权法（涵盖民事索赔，如疏忽或滋扰）或刑法（涉及非法行为和犯罪，如攻击、谋杀、入室盗窃或强奸）。如果一个化身袭击了另一个化身，是否可以将攻击和殴打的刑法适用于这种情况？我们怎样才能让化身为他们在元宇宙的行为负责呢？这将会很复杂，因为这意味着需要给化身赋予法律地位，让他们在法律体系中拥有权利和义务，允许他们起诉或被诉。这显然是很难做到的。此外，证明攻击或殴打也会更加困难，因为它通常需要“实际的身体伤害”。在元宇宙中，自然不会有实际的身体伤害。要证明化身所遭受的伤害、损失或损伤是很有挑战性的。〔20〕

其次，虚拟资产的确认和保护。元宇宙中的交易通常使用加密货币或 NFT（不可伪造的代币）。NFT 是一种独特的数字资产，它可以是一张图片、一段音乐、一段视频、一个三维物体，或其他类型的创意作品。很难说这是一种趋势还是一种新的和令人兴奋的资本投资形式。这些类型的交易提出了一些有意义的法律问题。〔21〕例如，在“现实”世界中，当涉及购买一件艺术品时，财产法规定，所有权针对的是实际的实物艺术品。买方可能拥有也可能不拥有艺术作品的知识产权，这取决于销售条款。但是，在数字艺术的交易中，买者所拥有的并不是实物艺术品。这种所有权究竟包括什么样的权利？是一种许可形式，还是一种服务？在这种情况下，真正的所有权可能仍然属于所有者。这可能意味着，没有真正所有者的许可，买方不能出售该物品。虚拟房地产也已成为一种 NFT，个人或者公司花费巨资在元宇宙中拥有某种“房地产”。现实世界的土地法能在这里适用吗？比如，现实世界的法律能否用于制止元宇宙中私人土地上的入侵者？这种“房地产”能办理抵押贷款吗？

再次，个人数据的隐私问题。元宇宙中另一个对法律的挑战是对数据的有效保护。元宇宙中化身间的互动将暴露出个人数据的多样性。这可能包括面部表情、手势和其他类型的反应。这些都需要有效的保护。欧盟的《通用数据保护条例》（GDPR）、英国的《数据保护法》已有相关规定。但是，鉴于元宇宙的新颖性，为了确保用户的权利得到保护，可能需要重新审视这些法律中有关数据处理的规定和程序。

最后，知识产权问题。互联网已经给音乐家、电影制片厂和软件业带来了大量的版权问题，而元宇宙也可能会有自己的一系列版权问题。根据美国法律，美国的版权保护适用于“固定在任何有形表达媒介中的原创作品”〔22〕。元宇宙的许多方面都有可能受到版权保护，如软件、图形、视频和音频记录。虽然元宇宙可能会给版权人提供保护，但也有潜在的风险和挑战。版权作品的盗版可能是一个问题，当版权作品的使用很少时，版权所有者在证明版权侵权时可能会遇到问题。

---

〔20〕 See Brandy Tricker, Taming the Wild West: Solving Virtual World Disputes Using Non-Virtual Law, 35 *Rutgers Computer and Technology Law Journal* 138 (2008).

〔21〕 See Ahad Syed, NFTs: Sharks and Shards: What Are Fractional Nonfungible Tokens and Are They Subject to Securities Regulation?, 110 *Illinois Bar Journal* 18 (2022).

〔22〕 See Copyright, LYNN University, available at https://www.lynn.edu/university-policies/volume-i-governance-and-administration/copyright-policy, last visited on Aug. 29, 2022.

商标在元宇宙中也可能是有效的。商标是一种知识产权，由文字、图形、字母、数字等要素组成，用于识别具有特定来源的产品或服务并将其与其他产品或服务区分开来。商标法防止未经授权的第三方以任何可能淡化商标的方式使用该商标。〔23〕如果有人创建了一个模拟现实世界的虚拟世界，里面有商店、餐馆和咖啡馆，并包括星巴克、Applebee's 之类的标志，这些品牌的商标所有人就有理由对创建该虚拟世界的实体提起诉讼，因为这将使一个理性的人相信商标所有人拥有或赞助这些虚拟企业。元宇宙为新形式的沉浸式娱乐提供了无限机会，包括游戏、电影、音乐、音乐会和节日。这意味着有关知识产权的法律和法规需要与时俱进，涵盖新的知识关系。

所有这些都使监管变得至关重要，尽管说到监管，人们尤其是内容创作者会感到紧张。需要监管的不仅仅是平台供应商，也包括消费者个人。

五、规范元宇宙的可能性

（一）主要研究路径

21 世纪初，随着虚拟游戏的发展，虚拟世界（virtual reality）引起了法律学者和从业者的注意，他们在各种背景下探究了虚拟世界与现实世界法律之间的关系，重点关注现实世界的法律可以或应该在多大程度上适用于虚拟世界活动，以及虚拟世界治理和争议解决的相关问题。〔24〕近年来国外出现了大量研究虚拟世界相关法律问题的文献，其研究进路包括：第一，现有“真实世界”的法律规则如何可能以及是否应该适用于虚拟世界。〔25〕这方面研究有的是描述性的，对现有“真实世界”法律是否确实适用于虚拟世界活动进行研究；有的是规范性的，探究现有“真实世界”法律是否应该适用于虚拟世界活动；有的两者兼而有之。第二，从虚拟世界的视角看待法律与虚拟世界的关系，从虚拟世界活动和争议开始，回望现有的“现实世界”法律学说或制度对虚拟世界治理〔26〕或解决虚拟世界争端的适切性。〔27〕第三，两个世界融合的视角。将虚拟世界视为“边界或边界空间”，参与者及其互动是在虚拟和现实之间来回穿梭，法律机构如何处理虚拟与真实之间的这种交叉融合，并说明两个世界的边界及其上出现的各种问题。〔28〕

另一个值得关注的研究进路，是从社会法律（socio-legal）的角度，探究虚拟世界本身和内部的合法性构建和执行，以及社会秩序的维护。研究法律与虚拟世界之间关系的最早作品之一，就是运用了社会法律/法律人类学的视角来构建虚拟世界中的合法性。〔29〕在《第二人生》中，法

〔23〕 See Theodore C. Max, Trademarks in the Veldt: Do Virtual Lawyers Dream of Electric Trademarks, 101 *The Trademark Reporter* 282 (2011).

〔24〕 See Jack M Balkin & Beth Simone Noveck eds., *State of Play: Law, Games, and Virtual Worlds*, New York University Press, 2006.

〔25〕 See Caroline Bradley & A Michael Froomkin, Virtual Worlds, Real Rules, 49 *New York Law School Law Review* 103 (2004).

〔26〕 See Michael Risch, Virtual Rule of Law, 112 *West Virginia Law Review* 1 (2009); Michael Risch, Virtual Third Parties, 25 *Santa Clara Computer and High Technology Law Journal* 415 (2009).

〔27〕 See Kevin W Saunders, Virtual Worlds—Real Courts, 52 *Villanova Law Review* 187 (2007).

〔28〕 See F Gregory Lastowka & Dan Hunter, The Laws of Virtual Worlds, 92 *California Law Review* 1 (2004).

〔29〕 See Eric M. Fink, The Virtual Construction of Legality: Griefing and Normative Order in Second Life, 21 *Journal of Law, Information and Science* 89, 90, 91 (2011).

· 11 ·

律和社会秩序问题表现得尤为明显。这些研究关注的重点不是现实世界法律与虚拟世界之间的连接，“真实世界”法律如何适用于（或是否应该适用于）虚拟世界活动，或者“真实世界”法律理论或机构如何适应虚拟世界治理和争议解决，而是虚拟世界居民自身对合法性的构建和体验。这种方法将虚拟世界社会关系作为一种新兴属性的社会规范和非正式秩序加以考察。

（二）虚拟世界的法律关系

对虚拟世界法律问题的研究很多是以《第二人生》为案例素材的。《第二人生》是一个在线虚拟世界或多用户虚拟环境，参与者通过化身参与常规的或非常规的线上活动，在虚拟空间实时与他人互动。其开发和运营者林登实验室（Linden Lab）将其描述为一个由居民创建的三维虚拟世界，自 2003 年向公众开放以来发展迅猛，如今全球数百万居民居住在这个虚拟世界中。在这个庞大的数字大陆上，充满了人、娱乐、体验和机遇，定居者在这里建造房子，进行创作并被他人的创作所包围。在这里数字创作的知识产权受到保护，居民之间可以进行买卖和贸易。该市场支持每月通过世界贸易单位林登币（Linden dollar）进行的数百万美元的交易，林登币可以在几个繁荣的在线林登币交易所兑换成美元。虽然《第二人生》在某些方面类似于多人电脑游戏，但它的特点在于，该活动是开放式的，而不是由特定的目标和角色驱动。此外，与大多数电脑游戏不同，《第二人生》明确允许并认可“真实货币交易”。

在《第二人生》的虚拟空间中，几乎可以遇到“真实”世界的每一个可以想象的合法和非法方面，但是明显缺乏一个重要的现实世界的特征，《第二人生》没有正式的法律制度，也没有解决居民之间纠纷的法律机制。然而，缺乏正式的法律体系并不意味着在《第二人生》中不会出现“法律问题”，这也是本文所关注和研究的基本问题。居民之间的互动和争议可能引发与不动产、动产和知识产权相关的问题，合同和商业交易、诽谤和隐私、公民权利和自由、犯罪与惩罚，以及其他各法律领域的问题。〔30〕巴尔金（Balkin）提炼了虚拟世界的六种基本关系：（1）平台所有者和国家之间的关系，关于游戏空间的设计、维护以及管理问题；（2）玩家和国家之间的关系，关于玩家参与游戏空间的规则；（3）玩家和平台所有者之间的关系，关于玩家和平台所有者在游戏空间的规则；（4）玩家之间关系，关于一方的游戏空间内的活动是否侵犯了另一方的合法权利；（5）平台所有者与未玩游戏的第三方之间的关系，关于游戏空间内的活动是否损害了第三方受法律保护的利益；（6）玩家和未玩游戏的第三方之间的关系，关于玩家的游戏空间内的活动是否损害了第三方受法律保护的利益。〔31〕

姆努金（Mnookin）描述了早期基于文本的虚拟世界 LambdaMOO 中发展起来的非正式规则体系和争议解决系统。在这个虚拟空间中，新规则将由全体居民投票表决，如果获得三分之二的多数票，则予以通过。虚拟空间中发生的纠纷和争议提交给有约束力的仲裁机构，仲裁员由居民自愿担任。姆努金研究发现，大多数纠纷都与虚拟世界中的产权和言论自由有关，虚拟世界的性质受到居民理解虚拟世界活动与现实世界法律之间的关系隐喻的影响，其将虚拟世界分为四种类型，即社交俱乐部、村庄、独立的国家和角色扮演游戏。在“社交俱乐部”的隐喻中，虚拟世界

〔30〕 See Benjamin Duranske, *Virtual Law: Navigating the Legal Landscape of Virtual Worlds*, American Bar Association, 2008.

〔31〕 See Jack M. Balkin, Law & Liberty in Virtual Worlds, 49 *New York Law School Law Review* 63, 67 (2004).

• 12 •

的活动本质上与现实世界的法律具有相关性。在“村庄”的隐喻中，虚拟世界被视为现实世界的一个子集，居民在尝试纠纷内部解决后，仍然可以寻求现实世界的法律救济。“独立国家”的隐喻则意味着一个充分发展的治理体系，独立于现实世界的法律体系。“角色扮演”隐喻将虚拟世界的活动视为一场游戏，除非虚拟世界的行为会造成现实世界的损害，现实世界的法律将不适用于虚拟世界。〔32〕

LambdaMOO 虚拟世界的建构无论是程序性的还是实质性的社会规范，都强烈依赖于现有法律模式，这表明了将虚拟现实视为与现实生活完全不同的范式的局限性。任何虚拟世界既不是完全自主的，也不是对现实世界法律的简单模仿，它是融合了现实世界的法律概念以及制度变化和创新理念的一种法律形式。这些隐喻在《第二人生》中具有相同的效果。虽然《第二人生》的居民通常会表达与“村庄”和“独立国家”的隐喻一样的情感，试图在《第二人生》中建立相对或完全自主的正式法律制度，在虚拟世界活动和“现实世界”规则之间保持鲜明的区别，但是迄今为止没有任何一个取得成功。〔33〕虚拟世界居民在缺乏正式法律体系和官方法律机构的情况下构建非正式规范秩序的方式，〔34〕值得进一步研究和探讨。虚拟世界与现实世界在法律关系上具有同一性、关联性和相似性，虚拟世界的规范秩序建构依赖于现实世界的法律概念、原则和制度。元宇宙与虚拟世界在构成和性质上有区别吗？元宇宙有哪些特殊的问题？以上研究为我们进一步观察元宇宙能否成为法学的研究对象，现实世界的法律应否适用于元宇宙提供了研究模板和参照对象。

（三）政府监管的可能性

世界各国政府在过去几十年里，通过政策和立法加强对互联网的规制和网络空间活动的控制，监管机构尝试为数字领域起草和实施规则。虽然数字版权管理（DRMs）以及其他类似的技术解决方案的结果记录好坏参半，但不可否认的是，对网络和虚拟空间的法律规制和监管争论是近年来围绕数字科技发展的主要事件和基本特征。对 2D 互联网最有效的政府监管方式是一种对门户进行的管制，虽然这种方式的最初意图是让 ISPs 对发布的内容负责，但这也推动了一系列的立法解决方案，其中包括对平台的责任豁免。〔35〕如果互联网能够受到私人实体和政府、国际机构的合理监管，那么元宇宙是否需要完全不同的监管方式？至少从目前对元宇宙的构想来看答案是否定的，大部分适用于网络空间的法律解决方案都可以适用于元宇宙。〔36〕

以管辖权为例，近年来最重要的信息法争议问题是将国家立法适用于国际数字媒体平台。在司法领域的主要障碍是试图确定法院如何以及何时对其他国家的法人和自然人行使管辖权。另一个问题是内容提供商是否应该受制于世界上所有的司法管辖区，因为他们的作品位于那个国家。虽然要回答和解决这些问题是困难的，但目前已经出现了解决该问题的立法方案和符合法律逻辑

〔32〕 参见前引〔29〕，Eric M. Fink 文，第 95 页。

〔33〕 See Greg Lastowka, *Virtual Justice: The New Laws of Online Worlds*, Yale University Press, 2010, p. 9.

〔34〕 参见前引〔29〕，Eric M. Fink 文，第 89－111 页。

〔35〕 See Ethan Katsh, Bringing Online Dispute Resolution to Virtual Worlds: Creating Process Through Code, 49 *New York Law School Law Review* 271 (2004).

〔36〕 See Andres Guadamuz, Back to the Future: Regulation of Virtual Worlds, 4 *A Journal of Law, Technology and Society* 242 (2007).

的司法判决。〔37〕

网络空间的争论转移到虚拟世界是否具有相同的意义？《第二人生》是否能够受到法律的约束？如果出现法律纠纷，是否可以向法院起诉？答案是肯定的。虚拟世界按照区域划分有三种类型：全球、区域和国家。全球每个人只要有账户和互联网就可以访问虚拟世界，例如《星战前夜》和《第二人生》。区域虚拟世界《魔兽世界》《英雄之城》和《天堂》的居民限定在某一特定地区或管辖范围内，即有明确的不同服务器之间内容的地理分隔。目前，区域性虚拟世界存在的原因主要有：在技术性方面，区域或国家服务器往往连接较少，可以更便宜的运行和维护；在语言方面，有些游戏可能需要对客户端进行语言的修改；在社会、文化方面，游戏可能没有全球性的吸引力，但玩家可能喜欢和说母语的人一起玩；在法律方面，通过拥有符合特定法规的区域服务器来减少潜在责任。

这些区域服务器的实施本身就是很好的例证，对虚拟世界的监管不仅是可能的，而且是现实的。用户必须建立账户才能参加游戏或进入虚拟环境，这可以限制从多个国家 IP 地址连接的用户，或提供商可以采取支付限制，即你必须在某个国家拥有一个银行账户才能创建该虚拟账户。这种对潜在用户的审查有助于通过最终用户许可协议［End-User License Agreements（EULAs）］、支付方式，甚至通过他们的互联网服务提供者将用户进行潜在身份识别和捆绑。〔38〕元宇宙带来的科技进步有可能再次改变进入虚拟世界的方式，引导和改变我们生活的某些方面，如当前热烈讨论的区块链技术导致的去中心化效应。然而，让人惊叹的新技术之美不应该让我们忽视这样一个事实，即政府通过技术创新、迭代和升级实现对社会的管控，既包括现实世界也包括虚拟世界。而法律规制和政府监管对虚拟世界来说是必需的，元宇宙也不例外。未来，我们可能像谈论网络空间一样谈论元宇宙，两者之间甚至可能没有任何区别。

（四）规范元宇宙的几个议题

1. 私权力的宪法规制

对私权力进行宪法规制可以追溯至 20 世纪 60 年代巴龙（Jerome A. Barron）发表在《哈佛法律评论》上的一篇重要文章，其标志了私权力宪法规制研究的开端。他关注对个人言论进行审查的私权力，认为对美国言论自由最大的威胁不是国家，而是大众媒体对个人言论的压制。〔39〕此后，学术界的讨论主要围绕传统媒体权力与法律规制，对表达自由进行控制的新媒体私权力形式和文化实践，国会立法和政府监管以及法院宪法解释对私权力与基本权利的权衡。21 世纪以来，大科技公司主导和推动了信息和数字技术的发展，由此形成的技术权力具有私权力的基本特征，形成了新的宪法权利和权力关系。数字平台的审查是附带性审查，具有与政府合作和融入的特征，数字平台责任是促进公私合作的一种策略，而美国私人平台责任豁免将导致新的宪法权利危机。新兴技术对社会的影响不仅是市场性的，而且是非市场性的，竞争法和反垄断法已经不足以应对上述挑战，传统的私法救济在面对私权力时凸显其理论困境。巴尔金认为，数字人权的保

〔37〕 See Dow Jones v. Gutnick［2002］HCA 56.

〔38〕 See Farnaz Alemi，An Avatar's Day in Court：A Proposal for Obtaining Relief and Resolving Disputes in Virtual World Games，11 *University of California Los Angeles Journal of Law and Technology* 1（2007）.

〔39〕 See Jerome A. Barron，Access to the Press—A New First Amendment Right，80 *Harvard Law Review* 1461（1967）.

障需要对私权力进行宪法规制。〔40〕

今天的互联网是几十年来通过政府研究实验室、大学、独立技术专家和机构的工作建立起来的。这些大多为非营利性的集体组织，通常专注于建立开放标准，帮助服务器共享信息，就未来的技术、项目和想法进行协作。任何人都可以从任何设备、任何网络上访问或构建互联网，成本很低甚至没有成本。然而，“企业互联网”是当前元宇宙的期望，元宇宙正由私营企业开拓和建设。2016年早在全世界企业高管认真考虑元宇宙之前，Epic Games的斯威尼（Sweeney）告诉VentureBeat：“如果一家中央公司获得元宇宙的控制权，他们将比任何政府都强大，它将成为地球上的神。”Nvidia创始人兼首席执行官黄仁勋（Jensen Huang）认为，元宇宙的GDP最终将超过“物质世界”。元宇宙的概念意味着我们生活、劳动、休闲、时间、财富、幸福和人际关系中越来越多的部分将在虚拟世界中度过，而不仅仅是通过数字设备来辅助生活。它将位于我们的数字和物理经济之上，并将两者结合在一起。因此，控制这些虚拟世界的公司将比当今数字经济中的领导者更具有统治力。〔41〕

元宇宙将使当今数字社会存在的诸如数据权利、数据安全、虚假信息、数字人权、平台监管等难题更加尖锐。在元宇宙时代处于领先地位的大科技公司的哲学、文化和优先事项将决定我们未来的世界。从宪法的角度来看，承认或者不承认像Meta这样的大公司的宪法地位，以及它是否有可能改变我们现有政治权力的结构，是一个重大的宪法问题。扎克伯格曾经明言，Facebook事实上更像一个政府，而不是传统意义上的公司。〔42〕Facebook有自己制定规则、自己执行、自己裁决的实践。此外，元宇宙与之前的虚拟世界的区别在于区块链，区块链在元宇宙中的应用有两个主题：虚拟货币和虚拟资产。未来元宇宙将发行自己的货币或者类似的凭证，现在的美国，比特币、各种代币、加密货币等等已经形成了初具规模的市场，实际上对美元形成了一定的冲击。当前热议的是区块链技术将产生去中心化效应，但也有学者对此持怀疑观点，区块链和元宇宙是不是一个共生关系，现在没有明确答案，关于虚拟资产区块链解决的仅仅是记账的问题，不能解决虚拟资产体现出的自身使用价值问题。更核心的问题是，本质上来讲元宇宙一定是中心化的，元宇宙的构建需要规则，那么这些规则都需要中心化才能实现。〔43〕这是一个宪法上应该考虑的问题。当然，更重要的宪法问题是，由于化身的普遍化，如何来界定“现实—虚拟”这种状态下的人的身份。传统宪法和宪法学考虑到的是自然人和法人（拟制的人），但是没有考虑过虚拟的人（virtual person）。研究者应在宪法层面提前关注化身和主人，虚拟人和现实中的真人之间的互动与调节，界定一个或数个化身与真人及他人（真人或化身）之间的法律关系。

在线视频游戏以及托管和营销游戏的平台带来的教训和风险是：如果不加以控制，私人公司

〔40〕 See Jack M. Balkin, Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation, 51 *University of California Davis Law Review* 1149, 1187 (2018).

〔41〕 参见前引〔13〕，Mathew Ball文。

〔42〕 See Henry Farell, Margaret Levi & Tim O'Reilly, Mark Zuckerberg runs a nation-state, and he's the king, Vox, available at https://www.vox.com/the-big-idea/2018/4/9/17214752/zuckerberg-facebook-power-regulation-data-privacy-control-political-theory-data-breach-king, last visited on Aug. 29, 2022.

〔43〕 参见前引〔11〕，贾韬文。

· 15 ·

和资本将以逐利为目的，把元宇宙带入危险的环境中。目前很多国家已经开始对元宇宙游戏系统进行立法规范。例如，《欧盟指令 2010/13》（Directive 2010/13 EU）修正案寻求将服务监管与线上电视视频相结合，包括特定的视频共享平台（VSP），以保护未成年人免受有害内容的影响。其他欧洲国家开始建立网络规制体系。18 岁以下儿童及青少年是新的英国《适龄设计规范》（ICO Age-Appropriate Design Code）关注的主要对象，该规范于 2021 年 9 月生效。该规范建议一定的默认程序设置，包括儿童个人数据处理服务的设计。一项新的德国法律《联邦青年保护法》（Jugendeschutzgesetz-JuSchG）于 2021 年 5 月 1 日生效，其立法目的在于保护儿童和年轻人免受新媒体消费的伤害，并且保证媒介的传播或获得是按照年龄分类而执行。各种类型的媒体和出版物涉及年龄分类，包括不道德和暴力内容、详细的暴力行为展示、大屠杀、获取正义的弱肉强食法则的建议等。法国也开始立法规范线上行为。一项待定的法国视听改革草案授予单一机构执行权力，视听和数字通信管理局［Audiovisual and Digital Communication Regulatory Authority（ARCOM）］被认为是新超级立法者，有能力规范在线平台、打击互联网有害内容、促进隐私保护。〔44〕而在所有国家的政策法律中都需要考虑的首要问题是，规范平台、开发商、投资者未能在平台上履行反线上有害内容义务时，应否承担责任以及如何承担责任。这些问题将在未来元宇宙时代继续呈现和发展。未来在很大程度上是不确定的，在建构元宇宙的过程中，谁来管控元宇宙是重要的议题，在宪法层面对元宇宙的私权力进行有效规制，对于塑造更美好的未来具有结构性的基础作用。

2. 个人数据保护

从数据保护的角度来看，未来元宇宙中 VR（virtual reality）技术进步和发展将涉及一些相关问题。VR 技术能够通过眼球追踪系统、面部识别系统和先进的传感器（如指纹、声纹、手和脸的几何形状、肌肉电活动、心率、皮肤反应、眼球运动检测、头部位置等）收集身体跟踪数据，为用户提供沉浸式和舒适的体验。尽管这项技术还没有完全投入大众市场，但已经出现了严重的隐私问题。与其他传统技术相比，VR 需要收集和处理越来越私密的个人数据，涉及欧盟 GDPR 的相关原则和规定。该类数据可被界定为生物识别数据（biometric data），即根据 GDPR 第 4（14）条，“与自然人的身体、生理或行为特征相关的特定技术处理产生的个人数据，能够确认该自然人的唯一身份，如面部图像或指纹数据”〔45〕。生物识别数据是一种特殊的个人数据类别，对它们的处理需要特别注意。GDPR 第 9 条规定除就业和社会保障法、至关重要和实质性的公共利益、预防或职业医学等某些有限目的外，禁止对生物识别数据（用于唯一识别自然人）进行处理，除非数据主体明确同意。〔46〕意大利数据保护局关于生物识别数据的一般申请令重申：处理生物识别数据需要提供信息通知；有关处理须得到数据主体的同意；生物特征数据必须通过适当的安全措施（例如加密）加以保护；含有生物特征数据的数据库必须能够访问和追踪；数据

〔44〕 See John Russel, *Metaverse For Beginners: A Complete Guide on How to Invest in the Metaverse, Copyright by John Russel*, 2022, pp. 37 - 40.

〔45〕 Art. 4 (14) GDPR, General Data Protection Regulation (GDPR), Definitions, available at https://gdpr.eu/article-4-definitions/, last visited on Jul. 22, 2022.

〔46〕 See Art. 9 GDPR, General Data Protection Regulation (GDPR), Processing of Special Categories of Personal Data, available at https://gdpr.eu/article-9-processing-special-categories-of-personal-data-prohibited/, last visited on Jul. 22, 2022.

必须保留至处理目的所需的时间。〔47〕其中，同意是生物识别数据收集处理的有效法律基础。衡量有效同意的核心是自愿原则，如果服务没有提供处理生物识别数据的有效替代办法，可以认为同意不是自愿的。值得注意的是，数据主体所谓的“虚拟隐私”在 VR 环境下可能与在非 VR 环境下不同，其隐私感知较现实世界低，事实上导致非自愿同意处理生物识别数据的情况比现实世界更为突出。因此，法律有必要严格规范 VR 处理生物识别数据，在数据主体没有任何有效的替代方案的情形下，认定该同意为非自愿，从而不能获得处理生物识别数据的许可。此外，VR 处理生物识别数据的必要性原则也应考虑在内，禁止或限制 VR 对个人生物识别数据的非必要使用和处理，对必要性原则在不同应用场景的适用规定条件和程序。根据 GDPR 第 25 条，默认/设计的隐私原则（privacy by default/design）要求产品/服务的设计和开发是为了保护用户的个人数据。特别是考虑到“处理大量生物识别数据对自然人的权利和自由造成不同风险的可能性和严重性”，VR 提供商应在处理数据时，实施适当的技术和组织措施，如匿名化和/或数据最小化，以满足 GDPR 的要求和保护数据主体的权利，并确保为特定目的处理个人数据的必要性。〔48〕根据 GDPR 第 35 条规定，VR 提供商在处理数据之前应进行数据保护影响评估［Data Protection Impact Assesement（DPIA）］。〔49〕随着数字技术的不断更新，包括 GDPR 在内的各国现有法律的有效适用必然会面临新的难题和挑战。在元宇宙背景下个人数据的跨境传输、未成年人数据的特殊保护、数据侵权责任归属及承担等与数据保护相关的一系列问题，都需要法律因应技术发展而做出跟进、改变和调整。

3. 刑法的适用问题

元宇宙中可能涉及的刑事犯罪，包括性骚扰、性侵犯、虚拟物/虚拟财产的盗窃、个人数据的盗窃、身份盗用、诈取、欺诈、洗钱和非法融资活动等。2016 年，一位名叫乔丹·贝拉迈尔的女性成为一次虚拟性侵的受害者，引发了法律界和虚拟现实界对虚拟行为造成实际伤害的可能性的思考。贝拉米尔后来写道，她对这起事件感觉是“真实的”并且遭到了“亵渎”。近日一名 21 岁女性受害者在 Meta 发行的《地平线世界》游戏中，创建了一个女性虚拟形象，遭到一位男性虚拟人物的“性侵”。另有媒体报道，一名日本游戏玩家阿基拉（Akira）在 VRchat 虚拟游戏中遭到其他虚拟玩家的性侵犯。〔50〕目前学界和实务界对此类事件如何定性尚不明确，存在争议。一种观点认为，身体未被触摸，也可以被判定为性骚扰，因为虚拟行为对人格和尊严的影响通常是确凿无疑的。另一种观点认为，“虚拟强奸”（virtual rape）目前很难被定义为真正的“强奸”。因为强奸罪一般要符合三个条件：行为违背被害人（一般指妇女）的意愿；行为人必须采取使妇女不能反抗、不敢反抗或不知反抗的手段，通常是暴力、胁迫或者其他手段；施暴人和受害人要

〔47〕 See Giangiacomo Olivi, Niccolo Anselmi & Claudio Orlando Miele, Virtual Reality: Top Data Protection Issues to Consider, 3 *The Journal of Robotics, Artificial Intelligence & Law* 141 (2020).

〔48〕 See Art. 25 GDPR, General Data Protection Regulation (GDPR), Protection by Design and by Default, available at https://gdpr. eu/article-25-data-protection-by-design/, last visited on Jul. 22, 2022.

〔49〕 See Art. 35 GDPR, General Data Protection Regulation (GDPR), Protection Impact Assessment, available at https://gdpr. eu/article-35-impact-assessment/, last visited on Jul. 22, 2022.

〔50〕 参见大千纪实：《“VR 侵害”频频发生？虚拟世界中的猥亵行为，受害者可以维权吗?》，载 https://baijiahao.baidu.com/s?id=1732160284422915432&wfr=spider&for=pc，最后访问时间：2022 年 8 月 29 日。

有实际的身体接触。就此次元宇宙“性侵”事件而言，“虚拟强奸”可能满足条件一，或可满足条件二，但是，条件三（即二者要有实际的身体接触）可能无从谈起。这是当前切实存在的现实法律困境。〔51〕从受害人的角度来看，虚拟性侵、猥亵或强奸的真实性是虚拟行为是否与现实世界刑法具有相关性的关键因素。虚拟现实的独特性在于用户的完全沉浸感，虚拟现实的目的是欺骗用户的大脑，让他们认为他们的虚拟体验是真实的。研究表明，在虚拟现实中被扇耳光的受试者会在皮肤、电导率和心率水平上有相应反应，就好像他们真的被打了一巴掌。〔52〕沉浸感（immersion）是虚拟现实与任何其他通信技术的区别，技术的发展会加强虚拟世界的沉浸感。随着现实和虚拟之间的界限变得模糊，用户对虚拟身体的感知将与真实身体攻击具有同样的心理反应。匿名、缺乏后果和游戏文化已经导致了虚拟世界中的无数性骚扰事件。相关研究数据显示，在 600 多名 VR 游戏受访者中，约有 49％的女性在虚拟空间受到过侵犯，包括语言猥亵和虚拟性侵，36％的男性受访者受到攻击和骚扰，这显然是一种新型网络暴力，其造成的创伤不亚于现实中的侵害。〔53〕

刑法对虚拟环境的干预是一项富有挑战性的法律改革。虚拟世界中的行为将不再停留在虚拟世界中，其行为后果及于现实世界。个人控制的化身在沉浸式虚拟环境中对另一个人控制的化身的行为造成了现实世界的实际损害，刑法应对此作出必要回应，考虑将现实世界刑法概念及原则与虚拟现实相结合，因为虚拟行为可以造成真正的伤害，行为人需要为其所操控的化身在虚拟世界的行为承担相应的法律责任。刑法为有效预防和惩罚这种伤害而采取的任何行动所应遵循的原则，必须能够处理将虚拟行为定为犯罪时所面临的复杂问题。归根结底，最重要的出发点是承认虚拟行为可能造成真正的伤害。这一原则可以作为未来处理元宇宙相关法律责任的法理基础。〔54〕对虚拟环境施加的任何监管都需要在政策法律上明确，沉浸式虚拟环境应该在社会中扮演角色，虚拟世界不应成为法外之地。当然，刑法干预只是规范虚拟行为可采取的众多选择之一。虚拟现实开发者也应该对惩罚违法者负责。实施了不法行为的用户可能会受到平台警告，在虚拟环境中面临处罚，或者被完全禁止进入该环境。一些平台已经引入了个人泡沫，如果一个用户干扰另一个用户的个人空间，他们就会从受害者的视线中消失。〔55〕计算机代码是一种可用于管理这些问题的规则形式。然而，平台或者元宇宙自治尚不足以规范严重违法或者犯罪行为，类似的见解可见于人工智能伦理的讨论。当虚拟世界的行为造成严重危害时，刑法的在场及出场是规范未来元宇宙有序发展的必要策略。这些原则也适用于未来可能在元宇宙中实施的其他违法或犯罪行为。

〔51〕 参见王小伟：《元宇宙“性侵”事件：如何在虚拟世界保护人的尊严》，载 https://baijiahao.baidu.com/s?id=1734239302666360393&wfr=spider&for=pc，最后访问时间：2022 年 7 月 22 日。

〔52〕 See Mark A Lemley & Eugene Volokh, Law, Virtual Reality, and Augmented Reality, 166 *University of Pennsylvania Law Review* 1051 (2018).

〔53〕 参见川味东子：《“VR”性侵事件！对于虚拟世界中的猥亵行为，受害人是否能维权?》，载 https://3g.163.com/dy/article/HADMKLFT05534KYC.html，最后访问时间：2022 年 7 月 23 日。

〔54〕 See Joshua Hansen, Virtual Indecent Assault: Time for the Criminal Law to Enter the Realm of Virtual Reality, 50 *Victoria University Wellington Law Review* 33 (2019).

〔55〕 See Katherine Cross, Sexual Assault Enters Virtual Reality, The Conversation, 10 November 2016, available at https://theconversation.com/sexual-assault-enters-virtual-reality-67971, last visited on Jul. 24, 2022.

· 18 ·

六、结　论

约翰·佩里·巴罗曾在1996年发表了《网络空间独立宣言》，警告世界各国政府不要干预网络空间的独立性。今天，当人们讨论元宇宙议题时，可以很容易地将元宇宙与网络空间联系起来，再次重温网络自由的倡议，并构想未来元宇宙自由。未来数字新技术似乎保证了一种完全不同的监管方式，去中心化成为当下热议元宇宙的主要话题。所谓的网络自由论者的论点假设未来新技术在基本方式上是开创性的，从而需要一个完全不同于现实世界的监管方式。属于这一阵营的人倾向于看到网络空间，现在是元宇宙作为一个独立的王国，不受过时法律规则的约束和规范。本文认为，元宇宙从本质上来说，是一个虚实融合的数字空间，依附并依赖于现实世界。元宇宙无限度自由仅仅是一种乌托邦的想象，数字无政府主义最终导致的是失序与混乱，互联网的发展也验证了这一点。未来元宇宙的构建不仅是技术创新和迭代发展的过程，更是一个组织化、规则化和秩序化的过程，以法律规则为核心的秩序建构必然是再中心化而不是去中心化。法学研究的任务是从元宇宙空间的法律规范视角，提炼元宇宙的可能法律议题，深化虚拟世界和现实世界的法律概念、原则和制度的一般性与特殊性讨论，防范元宇宙可能的法律风险，探索构建元宇宙健康有序发展的社会秩序。

Abstract: Although "metaverse" is a concept that lacks a clear definition, the vision and imagination of "digital existence" reveal various possibilities for human beings to enter into digital social forms. The direction of the development of the metaverse depends on the choices and constructions of human beings themselves. The metaverse itself is not a method, nor a technology, but a commercial concept that integrates the three main characteristics in human nature: gaming (play), gambling and human tendency of pursuing interest. These three characteristics of man form the core of the metaverse. The virtual world and the real world share sameness, relevance and similarity in legal relations, and the construction of the normative order of the virtual world relies on the legal concepts, principles and institutions of the real world. The future metaverse is an order construction process of organizing, regulating and ordering with legal rules as the core. Legal and government regulation are necessary for the virtual world. Who will control the metaverse is an important issue. Effective regulation of the private power of the metaverse at the constitutional level plays a structural and fundamental role in shaping a better future.

Key Words: metaverse, recentralization, virtual world

(责任编辑：赵　真　赵建蕊)

财经法学 No. 5，2022
pp. 20 - 34

元宇宙的法律规制

丁道勤*

内容提要：元宇宙是通过虚拟现实或增强现实等数字技术形成的现实虚拟世界交融共生的数字生态系统。元宇宙放大并复杂化了现实世界的众多法律问题，如持续性非自愿的个人敏感信息综合采集所带来的隐私个人信息保护挑战、海量数据实时交互处理和加密网络技术的广泛应用冲击了数据安全保护体系、用户生成内容方式（UGC）对内容作品的确权和知识产权权益分配机制提出新挑战、跨平台一键登录和互操作的竞争反垄断等问题，以及缺乏统一可信的数字身份体系、数据资产确权利用规则不明晰、NFT 金融安全风险突出等特殊问题。元宇宙法律规制应坚持现实世界法律框架都能直接映射适用于元宇宙的基本原则，建议修订完善现有个人信息保护、网络数据安全及知识产权规则，延展制定元宇宙隐私个人信息保护的特别条款、数据全生命周期安全可信规范和 UGC 新的知识产权授权规则等。推动出台数字身份国家战略，通过数字身份专门立法建立统一分层次的数字身份体系，制定数据资产新的确权利用法律规则，从国家层面建立起统一的 NFT 监管框架。

关键词：元宇宙　数字身份　数据资产　非同质化代币（NFT）

元宇宙概念发端于《雪崩》，出圈于《头号玩家》《失控玩家》，爆火于被众多媒体称为“元宇宙元年”的 2021 年，更是在 2021 年 10 月 Facebook 更名为 Meta 后，引发全球行业追捧新热潮。元宇宙被描绘为不同于现实世界的另一个世界的蓝图，但元宇宙的内涵和外延仍是仁智互见，目前并没有统一的认知和概念。

从发展历程来看，互联网经历了三次重大变革时代。第一次是桌面互联网时代，即计算机普及带来桌面互联网，自 1971 年首款个人计算机（PC）诞生以来，其应用领域从科学研究、政府机构逐步走向家庭。到 20 世纪 90 年代互联网大发展，诞生了 IBM、微软、雅虎、谷歌、新浪、

* 丁道勤，北京航空航天大学工业和信息化法治战略与管理（工信部）重点实验室研究员。
本文仅为个人观点，不代表任何机构立场。

搜狐等大门户网站。第二次是移动互联网时代，标志是 2007 年第一代 iPhone 发布，加速智能手机普及，开启移动互联网时代。特别是 2010 年后，3G、4G 驱动移动互联网大发展，全面颠覆人们的生活、体验以及价值认知，如网络购物、本地生活服务、手机游戏、移动社交等，诞生了 Facebook、Twitter 及国内的 BAT 等互联网公司。第三次是下一代互联网，如未来更加先进的 AI、XR、大数据、云计算等都将围绕 5G 和 6G 产生变革，元宇宙正处于第三次互联网技术变革时期。

元宇宙承载了人类数字化转型的愿景，但技术变革的同时也带来了众多问题，例如，技术问题、经济问题、道德伦理问题、法律问题、社会治理问题，也引起社会各界的广泛关注。在元宇宙被热炒的当下，尤其需要冷静理性探究元宇宙本源法律问题。那么，元宇宙究竟有哪些特殊法律问题，是否为“法外之地”，又该建立怎样的法律规制体系，值得深入思考。本文尝试分析元宇宙的关键属性，探讨元宇宙带来的复杂性和特殊性法律问题，进而提出相关法律规制建议。

一、元宇宙的特性

从词源上看，metaverse 有两个部分：meta 源于希腊语，有“元”的意思，“元”意指最基础、最本源。verse 是指 universe，有“宇宙”的意思。因此，metaverse 被顺理成章地翻译为了“元宇宙”。科幻小说《雪崩》中描绘了一个称为元宇宙（metaverse）的多人在线虚拟世界，用户以自定义的“化身”（avatar）在其中进行活动。〔1〕维基百科对元宇宙的描述是：通过虚拟增强的物理现实，呈现收敛性和物理持久性特征的，基于未来互联网，具有链接感知和共享特征的 3D 虚拟空间。元宇宙大致是生活在现实物理世界的自然人以“化身”或者“数字人”的方式，通过计算机操作系统，与其他数字人即时互动的 3D 数字虚拟空间，也是大部分人所认定的下一代互联网形态。〔2〕根据中纪委官网文章的定义，元宇宙是基于互联网而生、与现实世界相互打通、平行存在的虚拟世界，是一个可以映射现实世界、又独立于现实世界的虚拟空间。〔3〕综上，元宇宙是通过虚拟现实或增强现实等数字技术形成的现实虚拟世界交融共生的数字生态系统。

（一）关键特性

元宇宙的出现可能改变人类社会对于“自身存在”的主流认知，向虚拟时空的迁跃是信息技术和人类文明发展的必然趋势。作为人类社会的平行数字时空，著名分析师马特乌·波尔（Matthew Ball）认为，metaverse 具有永续性、实时性、无准入限制、经济功能、可连接性、可创造性六大特征，metaverse 不等同于“虚拟空间”“虚拟经济”，或仅仅是一种游戏抑或 UGC 平台。在元宇宙里将有一个始终在线的实时世界，有无限量的人们可以同时参与其中。它将有完整运行的经济、跨越实体和数字世界。Roblox 首席执行官大卫·巴斯祖可（Dave Baszucki）认为，元

〔1〕 参见〔美〕尼尔·斯蒂芬森：《雪崩》，郭泽译，四川科学技术出版社 2018 年版。

〔2〕 See Haihan Duan，Zhonghao Lin，Jiaye Li，Xiao Xu，Sizheng Fan & Wei Cai，Metaverse for Social Good：A University Campus Prototype，Proceedings of the 29th ACM International Conference on Multimedia，2021，pp. 153－161.

〔3〕 参见管筱璞、李云舒：《元宇宙如何改写人类社会生活》，载 https://www.ccdi.gov.cn/toutiaon/202112/t20211223_160087.html，最后访问时间：2022 年 6 月 7 日。

宇宙是一个将所有人相互关联起来的 3D 虚拟世界，人们在元宇宙拥有自己的数字身份，可以在这个世界里尽情互动，并创造任何他们想要的东西。归纳起来，元宇宙具备可靠的经济系统、强认同的虚拟身份、强社交性、开放自由创作、沉浸式体验等特点。从功能层面，元宇宙是一个承载虚拟活动的平台，用户能进行社交、娱乐、创作、展示、教育、交易等社会性、精神性活动。〔4〕综上，元宇宙的关键特征主要表现为沉浸式体验、强社交性、全息生存、自由创造、经济系统等。

（二）技术架构

元宇宙是 AI、区块链、5G、物联网、半导体、显示等技术的集大成者。业界普遍认为，元宇宙是基于 Web 3.0 技术体系和运行机制的数字空间。从科学角度，元宇宙实质上就是广义网络空间，在涵盖物理空间、社会空间、赛博空间以及思维空间的基础上，融合多种数字技术，将网络、软硬件设备和用户聚合在一个虚拟现实系统之中，形成一个既映射于、又独立于现实世界的虚拟世界。从技术角度，元宇宙不宜称为新技术，而是现有 IT 技术的综合集成运用，它是信息化发展的一个新阶段。〔5〕总之，现阶段元宇宙实则是智能化信息技术的一种集成创新应用生态。

有专家认为，元宇宙的计算基础可以用 BIGANT（“大蚂蚁”）来概括，B 是指区块链技术（blockchain），I 指交互技术（interactivity），G 指电子游戏技术（game）、A 指人工智能技术（AI），N 指网络及运算技术（network），T 指物联网技术（internet of things）。〔6〕也有专家认为，元宇宙框架为硬件入口、基础设施、底层技术、人工智能、内容、合作方六大组件，首先是提供元宇宙体验的硬件入口（VR/AR/MR/脑机接口），其次是支持元宇宙平稳运行的基础设施（5G/算力与算法/云计算/边缘计算）与底层技术（引擎/开发工具/数字孪生/区块链），再次是元宇宙中的人工智能，最终呈现为百花齐放的内容，以及元宇宙生态繁荣过程中涌现的大量提供技术与服务的合作方。〔7〕也有人认为元宇宙并不是游戏的升级版，而是 BAND（blockchain、game、network、display）各技术赛道的融合，BAND 构建了元宇宙的四大技术支柱，即区块链（blockchain）、游戏（game）、网络算力（network）和展示方式（display），分别从价值交互、内容承载、数据网络传输及沉浸式展示融合构建元宇宙。〔8〕还有专家认为，元宇宙本身的核心技术归类为两类半。一类是感知与交互技术，即“脑机接口”，现在用的 VR、AR 的设备，在某种程度上可以理解为广义的脑机接口。第二类是持久计算技术，即可以支撑持久存在的虚拟世界的技术，包括相关的计算基础设施、引擎与建模技术等。还有半类核心技术是虚拟资产，是对元宇宙有益的补充和助力，但并不是非有不可。〔9〕

（三）主要场景

元宇宙拓展了游戏娱乐行业，并与更多的实体行业进行交互延伸，最终形成虚拟现实世界的

〔4〕 参见宋嘉吉、赵丕业：《元宇宙：互联网的下一站》，国盛证券研究报告，2021 年 5 月 30 日。

〔5〕 参见王文喜等：《元宇宙技术综述》，载《工程科学学报》2022 年第 2 期。

〔6〕 参见赵国栋、易欢欢、徐远重：《元宇宙》，中信出版社 2021 年版，第 26－28 页。

〔7〕 参见焦娟：《科技巨头布局元宇宙系列报告 1：Facebook，改名为 Meta》，安信证券研究报告，2021 年 10 月 29 日。

〔8〕 详见前引〔4〕，宋嘉吉等文。

〔9〕 参见袁昱：《全球视野下的元宇宙全景与展望》，载 https://mp.weixin.qq.com/s/3aE2Yef6c2BwfBUPeb_gpQ，最后访问时间：2022 年 6 月 7 日。

· 22 ·

交融一体，其主要应用场景有以下三大类：一是生活消费场景，主要包括游戏、虚拟社交、电竞、娱乐、智慧教育、医疗健康等，例如，Unity 和 Roblox 两大游戏制作平台让数百万创作者参与创作元宇宙游戏。二是经济生产场景，主要包括沉浸式电商、协同生产、工业数字孪生。三是协作空间场景，主要包括远程办公、全息虚拟会议、协作设计空间、虚拟地产、虚拟场馆、数字文旅等。

二、元宇宙的特殊法律问题

与桌面互联网和移动互联网时代一样，技术创新往往会推动监管创新，元宇宙相关产业在国内发展的潜在风险和法律问题，也引起相关监管部门的关注和警示。2021 年 11 月 19 日，新华社发文解码元宇宙指出，元宇宙在发展过程中，也将遇到价值伦理、虚拟空间管控等新问题，需要监管部门进一步进行规范。〔10〕2021 年 12 月 23 日，中纪委官网文章指出，目前元宇宙产业还处于发展初期，距离大规模产品化还十分遥远。元宇宙产业具有新兴产业的不成熟、不稳定等特征，还存在一些潜在风险。技术生态和内容生态尚未成熟，场景入口也有待拓宽，理想愿景和现实发展间仍存在漫长的“去泡沫化”过程。〔11〕2022 年 2 月 18 日，处置非法集资部际联席会议办公室（银保监会）发布《关于防范以“元宇宙”名义进行非法集资的风险提示》进行风险提示，一些不法分子蹭热点，以“元宇宙投资项目”“元宇宙链游”等名目吸收资金，涉嫌非法集资、诈骗等违法犯罪活动。元宇宙带来了先前未曾考虑到的新挑战和新变量，现实世界和互联网相关法律法规并不能覆盖元宇宙引发的所有问题。根据新技术新业务带来法律关系的调整、相关法律问题是否为元宇宙所特有为标准，元宇宙相关法律问题可以区分为映射延展问题和特殊性问题两个层面。

（一）映射延展问题

现实世界、桌面互联网和移动互联网现有的和众多悬而未决的法律问题，同样能映射和延展至元宇宙场景，并可能被放大而更加复杂化，例如，网络空间主权、内容安全、道德伦理、隐私个人信息保护、网络数据安全、知识产权、反垄断、刑事违法犯罪、税收等。这些问题并非元宇宙所独有，而是现实世界和互联网存在的法律问题映射到元宇宙场景之中。

其一，持续性非自愿的个人敏感信息的综合采集所带来的隐私和个人信息保护挑战。元宇宙是基于扩展现实技术向用户提供更真实的、沉浸式体验，意味着可能需要收集或导入更多的用户可识别信息，比如生物信息，这些个人敏感信息一旦泄漏或滥用，将对用户乃至整个元宇宙生态带来极大的隐患和冲击。有人甚至认为，元宇宙中无隐私，元宇宙是隐私荒地（privacy wasteland），〔12〕元宇宙将加工一些新类型的个人数据，包括面部表情、手势和其他分身在元宇

〔10〕 参见胡喆、温竞华：《什么是元宇宙？为何要关注它？——解码元宇宙》，载 http://gd.news.cn/newscenter/2021-11/20/c_1128081990.htm，最后访问时间：2022 年 5 月 24 日。

〔11〕 参见前引〔3〕，管筱璞等文。

〔12〕 See Edvardas Mikalauskas, Privacy in the Metaverse: Dead on Arrival?, available at https://cybernews.com/privacy/privacy-in-the-metaverse-dead-on-arrival/, last visited on Jun. 2, 2022.

宙交互时产生的反应。为了确保用户数据权利得到保护，关于数据处理的告知同意程序可能需要重新思考。〔13〕AR/VR 之所以带来了全新的用户隐私考量是因为：一是 AR/VR 设备由不同的信息收集技术组成，每一项技术都呈现出不同的隐私风险及相应的降低风险的方法；二是 AR/VR 设备收集的信息类型是其他一般消费者技术设备不收集的敏感信息；三是这种综合的信息收集对于 AR/VR 设备的核心功能至关重要。〔14〕因此，元宇宙场景中所使用数据的存储、处理和保护问题，以及数据被盗或滥用的责任问题，都是值得关注和亟待解决的。

其二，海量数据实时交互处理和加密网络技术的广泛应用冲击了数据安全法规的严格约束。元宇宙可能面临网络安全违规风险，如企业间谍、勒索软件攻击、国际网络战和老式黑客攻击都将转移到元宇宙。〔15〕元宇宙内不同应用之间、元宇宙和外部设备间的数据交互过程，以及外部设备采集、存储、处理、分发、利用和处置个人行为数据的过程，在技术层面上需要区块链相关的分布式网络、共识机制、智能合约、隐私计算等加以支撑，在法律层面上则需要受到数据安全相关法律法规的严格约束。〔16〕元宇宙中流通的海量数据以及这些数据的使用方式对用户构成了越来越大的安全风险，犯罪分子可以隐藏在加密及无法追踪的网络技术应用后面从而难以被识别并进行法律追踪，身份盗用、化身复制和滥用的风险为互操作性也带来了相应问题。〔17〕此外，元宇宙场景下的深度伪造内容（deepfake）带来的“非同意色情”、虚假新闻、名誉破坏、敲诈勒索、虚假证据、恶意商业竞争、负面社会消息、恐怖主义等现象引发对个人和社会两个层面的危害。〔18〕

其三，用户生成内容方式会对内容作品的确权和知产权益分配机制提出新挑战。元宇宙与桌面互联网和移动互联网很大的不同在于，元宇宙场景下的 UGC 方式，UGC 全称为 user generated content，也就是用户生成内容，即用户原创内容。UGC 的概念最早起源于互联网领域，即用户将自己原创的内容通过互联网平台进行展示或者提供给其他用户。第三方自由创造的内容，以及闭环经济体的持续激励，是元宇宙延续并扩张的核心驱动力。〔19〕元宇宙是一个交互平台，服务协议条款很可能允许用户对其个性化制作的分身和数字资产拥有知识产权。〔20〕在虚拟世界中创新是一个常态。2003 年，《第二人生》（一款游戏）没有采取行业惯例的做法，拒绝对其虚拟世界中生成的内容主张所有权，未来的游戏很有可能跟随这一做法。《第二人生》将版权所有权赋予了用户，这引发了版权法在虚拟创作上的适用问题。一方面推动传统版权法原则适用于虚拟世界引发了一系列问题，威胁创新，另一方面要求玩家转让其对虚拟作品的权利会抹杀

〔13〕 See Jerameel Kevins, Metaverse as a New Emerging Technology: An Interrogation of Opportunities and Legal Issues: Some Introspection, SSRN (March 6, 2022), available at https://ssrn.com/abstract=4050898, last visited on May 28, 2022.

〔14〕 See Pavan Duggal, *The Metaverse Law*, Kindle Edition, 2021, pp. 32 - 33.

〔15〕 See Jon M. Garon, Legal Implications of a Ubiquitous Metaverse and a Web3 Future, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4002551, last visited on Jun. 15, 2022.

〔16〕 参见董月英：《从法律视角看元宇宙发展的六个问题》，载《上海证券报》2022 年 2 月 17 日，第 8 版。

〔17〕 See European Parliamentary Research Service, Metaverse: Opportunities, Risks and Policy Implications, PE 733.557 - June 2022, available at https://www.europarl.europa.eu/at-your-service/en/stay-informed/research-and-analysis, last visited on Jun. 28, 2022.

〔18〕 参见华劼：《深度伪造内容著作权侵权问题研究》，载《电子知识产权》2022 年第 4 期。

〔19〕 参见前引〔6〕，赵国栋等书，第 103 页。

〔20〕 参见前引〔15〕，Jon M. Garon 文。

版权法所蕴含的激励机制。必须在鼓励创作和公共可获取性之间达成平衡，因为阻碍虚拟创新将威胁到虚拟世界自己的活力。〔21〕元宇宙带来了更多的挑战，即关于信息表达和虚拟创造是否受到法律保护、是否赋予所有权，在第三方信息层下方的支撑性内容是否属于修订或衍生作品的范围，引用或私人复制形式的著作权保护例外应如何适用的问题。〔22〕此外，元宇宙的知识产权问题还可能表现为擅自使用他人虚拟人形象，虚拟店铺中使用他人商标，侵犯他人受版权保护的游戏软件、角色、用户界面，数字资产是否具有《商标法》项下的商标资格，元宇宙应用的算法是否属于《专利法》保护的客体范围，以及知识产权侵权人身份不明时应向谁主张侵权责任等方面。

其四，跨平台一键登录和互操作的竞争反垄断问题。2020 年，Facebook 将其旗下的 Oculus 与 Facebook 账号绑定，要求用户用 Facebook 账户登入，连接社交和 VR 设备的数据，引发了德国联邦卡特尔办公室（FCO）的关注，FCO 主席认为，将 VR 产品和集团社交网络连接在一起可能构成滥用市场支配行为。〔23〕FIDO 联盟可通过没有密码的一键式登录、数据可自由携带、跨平台登录、互操作等方式，打破头部平台对数据账号和账户数据的控制权。延伸到业务领域，就可能出现利用垄断优势滥用信息的情况，从而产生垄断问题。此外，元宇宙很有可能出现平台经济中的自我优待问题，从 GAFA 的自我优待和反竞争行为可以看出，元宇宙平台可能优待自家产品，实施反竞争行为。〔24〕

（二）特殊问题

元宇宙的特殊问题主要表现为数字身份、数据资产、非同质化代币（NFT）。数字身份是元宇宙的起点和基石，基于数字身份及其身份行为产生的相关数据，积累于数字世界上的个人数据账户中，并进行挖掘、加工和增值利用，形成用户个人数据资产。用户再通过投资、创作、交易买卖形成数字化资产，典型的如通过记录各类数字资产权属的价值等价物的 NFT，搭建和丰富元宇宙的经济系统。

其一，缺乏统一可信的数字身份体系。元宇宙是承载人类虚拟活动的平台，是承载真人意识的数字体验，其核心在于可信地承载人的社交身份和资产权益。〔25〕Roblox 首席执行官大卫·巴斯祖奇（Dave Baszucki）指出，元宇宙的第一个关键特征是“身份”，且这种身份是可以自由设定并开发其“第二人生”的。〔26〕用户可以创建数字化身，以数字人或虚拟人身份在元宇宙进行生存、交互。数字化身代替了文本性的自我描述，个人可以在网络中通过替身的建构来获得身份，即在既定环境中形成他们的视觉形象、技能和态度以及他们的社会互动。因此，数字化身也

〔21〕 See Matthew R. Farley, Making Virtual Copyright Work, 41 (1) Golden Gate Univer Law Review 1, 1-32 (2010).

〔22〕 See Sophie Goossens, Christine Morgan, Cem Kuru, Fred Ji & DJ Cespedes, Protecting Intellectual Property in the Metaverse, 33 (9) Intellectual Property & Technology Law Journal 11, 11-16 (2021).

〔23〕 See Mason Marks, Biosupremacy: Big Data, Antitrust, and Monopolistic Power over Human Behavior, 55 UC Davis Law Review 513, 513-590 (2021).

〔24〕 参见前引〔15〕，Jon M. Garon 文。

〔25〕 参见前引〔4〕，宋嘉吉等文。

〔26〕 参见李章虎：《浅析“元宇宙”可能带来的法律挑战和解决路径》，载 https://mp.weixin.qq.com/s/czaepbduY-EY680kUKIzug，最后访问时间：2022 年 6 月 13 日。

被定义为一种用户交互式的社会表征。〔27〕元宇宙的核心在于增强“交互”，本质是用户肉身的数字化，并非用户肉身向元宇宙中“移民”。数字化身背后是元宇宙建设及其问题的起点与归宿——数字身份。〔28〕

数字身份作为数字主体的虚拟标识，关联了与该主体相关的属性信息，是其进行各种网络活动的支撑手段。数字身份管理是数字世界安全事务的核心，为鉴别、授权、访问控制、账户访问及其他各种与用户属性相关的应用提供支持。〔29〕用户的“身份”通过加密散列和时间戳记构成的分布式文件传输和存储系统，将得到前所未有的强化，甚至可以通过追溯政府颁布的出生证明、学历注册、工商登记和职业资格认证等信息，进行“盖戳”加密与固化，只能添加，不可篡改。而基于用户“身份”的一系列网络行为轨迹，例如图文与视频的发布、网购记录、大宗买卖、水电账单、商业合同、法证收集、生产供应链流程衔接等，都会通过属于每一个“身份”的资产通证（token）和智能合约运作，得到清晰的记录和戳记，甚至被智能合约自动推进。〔30〕当一个用户在元宇宙上通过化身进行交互时，如何确定所交互化身的准确性或合法性，元宇宙身份信息的可信认证研究就成为重要问题。〔31〕但是，目前我国尚没有建立起顺应数字时代发展的统一的可信数字身份体系。

其二，数据资产确权利用规则不明晰。在元宇宙里内容创作者是驱动经济发展的主要动力，元宇宙这种对现实世界底层逻辑的复制，让元宇宙成为坚实的平台，任何用户都能参与创造，且劳动成果受到保障。基于此，人们在元宇宙的劳动创作、生产、交易和在实际生活中的劳动创作、生产、交易没有区别。〔32〕用户基于个人数字身份，在数字世界中享受各类数字服务时，其在所有互联网平台上产生的本人相关的身份、行为、消费偏好、社交关系等所有数据都被关联起来，这些数据积累于各个平台的个人数据账户中。元宇宙更核心的问题可能是数据资产的确权问题，Web3.0 与 Web2.0、Web1.0 最大的不同在于，它是一个数据资产被确权的网络。〔33〕用户所产生的每个字段或轨迹信息，都可以进行定价，可以作为用户的虚拟财产进行确权。用户个人数据是数字世界的基石，以数据为生产要素的互联网服务提供者能够提升和改进现有的产品和服务，从而产生价值，也使得其所积累的数据得以变现，这就会衍生出数据流通利用的问题。因此，个人数据资产的核心问题在于个人数据如何关联、如何确权以及如何处置。

数据权属是数据利用和流通及数据产业化的逻辑起点，数据资产所有权的归属决定着数据价值利益的分配以及对数据质量、安全责任的划分。〔34〕数据确权和流通利用规则，在移动互联网

〔27〕 参见陆青：《数字时代的身份构建及其法律保障：以个人信息保护为中心的思考》，载《法学研究》2021 年第 5 期。

〔28〕 参见陈吉栋：《超越元宇宙的法律想象：数字身份、NFT 与多元规制》，载《法治研究》2022 年第 3 期。

〔29〕 参见国家质量监督检验检疫总局、中国国家标准化管理委员会：《信息安全技术 鉴别与授权 数字身份信息服务框架规范》（GB/T 31504—2015），引言。

〔30〕 参见骆轶航：《为什么 Web3.0 革命必将发生在中国?》，载 https://mp.weixin.qq.com/s/zEq6-CcyhjOb4Vyn4BngCw，最后访问时间：2022 年 6 月 14 日。

〔31〕 参见前引〔14〕，Pavan Duggal 书，第 19 页。

〔32〕 参见前引〔4〕，宋嘉吉等文。

〔33〕 此为万向区块链董事长兼 CEO 肖风先生的发言观点，有关数据资产的确权、授权和处置，笔者颇受启发，在此表示感谢。

〔34〕 参见丁道勤：《基础数据与增值数据的二元划分》，载《财经法学》2017 年第 2 期。

时代很难较好解决，但在元宇宙虚拟主体的场景下，就有可能得到解决。因为 Web3.0 商业模式的愿景和本质是在区块链上实现数据的确权，用户由此可以拥有、控制其在互联网上创造的数据并从中获利。〔35〕早在 1999 年，美国学者劳伦斯·莱斯格（Lawrence Lessig）教授系统提出数据财产化（data propertization）理论，他认为，应认识到数据的财产属性，通过赋予数据以财产权的方式，来强化数据本身的经济驱动功能，以打破传统法律思维之下依据单纯隐私或信息绝对化过度保护用户而限制、阻碍数据收集、流通等活动的僵化格局。〔36〕也有经济学者认为，在元宇宙中，用户应对其创造物享有所有权，企业应对虚拟财产享有所有权，以实现融资。例如，多角色扮演游戏（MMORPG）玩家在游戏中进行定制和创作，并将其中价值转换回现实世界。MMORPG 游戏证明，虚拟商品可以在现实世界具有相应价值，任何希望将用户引导到元宇宙的平台都必须允许用户赚钱，必须允许用户拥有其创造物，所有权是一个至关重要的问题。〔37〕现代虚拟世界运营的核心在于财产系统，这一系统具备现实世界的相同特征，如排他性的所有权、权利的存续、合同或强制条款的转让、货币系统。虚拟财产和其他无形、有时效的现实财产性权益之间几乎没有差异，不能因为虚拟财产并不“真实”而忽略虚拟财产的财产性权益。不论是边沁的功用主义，还是洛克的劳动论、黑格尔的人格论，都可以支持虚拟主体所主张的财产构成现实财产这一结论。〔38〕

其三，NFT 金融安全风险问题突出。非同质化代币（NFT）是表示数字或物理资产的所有权的数字证书，是数字资产的新形式，具有稀有和唯一性、不可篡改性、所有权可管理等特点。NFT 最早是在 2014 年为数字图像创建的，主要依赖区块链、NFT 市场平台、数字钱包等技术。〔39〕区块链是元宇宙的补天石，保障用户虚拟资产、虚拟身份的安全，实现元宇宙中的价值交换，并保障系统规则的透明执行。Web3.0 运动的领导者专注于找回因 Web2.0 而失去的财产权，通过使用 NFT 来强制执行财产、实现用户直接控制，以阻止企业过度扩张，Web3.0 可能矫正 Web2.0 的不平衡。〔40〕元宇宙独有的经济体系有可能会出现货币安全、金融诈骗等一系列问题。现阶段，除比特币外，NFT 是关键组成部分，其使得用户可以拥有、交易、购买、出售元宇宙资产和服务。NFT 记录了各类数字资产的创建和所有权，并将它们存储在区块链分布式账本中，该账本不可更改地分布在众多区块链用户之间，因此这些 NFT 记录不会发生单个结点故障。与所有权相关的这些创建和交易记录，使得每个 NFT 及相关艺术品或数字资产都是独一无二的，具有稀缺性和收藏价值。〔41〕因此，目前 NFT 主要应用于数字艺术藏品、虚拟房地产、游戏、供应链追

〔35〕 参见卢璟、夏彦、曾铮：《Web3.0 时代：数据保护法规将如何影响市场发展?》，载 https://www.toutiao.com/article/7107499463685538339/，最后访问时间：2022 年 6 月 19 日。

〔36〕 参见龙卫球：《数据新型财产权构建及其体系研究》，载《政法论坛》2017 年第 4 期。

〔37〕 See Cory Ondrejka，Escaping the Gilded Cage：User Created Content and Building the Metaverse，available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=538362，last visited on Jun.28，2022.

〔38〕 See F. Gregory Lastowka & Dan Hunter，The Laws of the Virtual Worlds，92（1）*California Law Review* 1，1-73（2004）.

〔39〕 参见美国政府问责局（GAO）：《NFT 概念、应用、风险、机遇和挑战》，载 https://www.gao.gov/assets/gao-22-105990.pdf，最后访问时间：2022 年 6 月 21 日。

〔40〕 参见前引〔15〕，Jon M. Garon 文。

〔41〕 See Michael D. Murray，Ready Lawyer One：Lawyering in the Metaverse，available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4082648，last visited on Jun.28，2002.

踪、健康医疗记录等领域。

对于 NFT 的法律性质，有“虚拟财产”和“权益凭证”等不同认识，〔42〕司法实践中多认定其为法律意义上的财产，例如，2022 年 6 月 6 日，纽约最高法院批准了一家总部位于美国的律师事务所“Holland & Knight”的申请，空投了 NFT 作为“服务通证”用于向被指控为黑客的被告发出临时限制令。在本案中，如果钱包所有者即被告未能在 30 天内对通知作出答复，案件将继续进行，法院可能将视为钱包所有者承认有罪，允许冻结被盗的数字资产。〔43〕2022 年 3 月，英国英格兰和威尔士高等法院裁定，NFT 构成法律意义上的财产，遭遇 NFT 被盗的权利人可向法院申请禁令，要求冻结相关账户，并强迫披露账户持有者信息。〔44〕新加坡法院与英国法院观点一致。2022 年 5 月 13 日，新加坡高等法院将 NFT 视为法律意义上的财产加以保护，发布禁令，在所有权争议纠纷解决之前，冻结以太坊链上的 Bored Ape Yacht Club NFT 作品的销售。〔45〕我国杭州互联网法院判决认为，NFT 交易的数字作品属于法律意义上的财产，NFT 数字作品交易行为受信息网络传播权控制，NFT 数字作品交易平台负有知识产权初步审查义务。〔46〕

NFT 交易可能引发以下特殊问题：一是 NFT 艺术作品的权属问题。NFT 所有者对其持有内容的权利范围有多大？在涉及知识产权的情况下，NFT 所有权是否本质上属于一种许可，作品所有权仍然归属主人，卖家在未取得主人同意的情况下不得销售作品？〔47〕如果艺术作品由多个匿名用户的分身完成，确定创作者的身份很难，在此情况下，法院如何认定合理使用？二是 NFT 房地产资产的权属。当虚拟房地产成为 NFT，用户和公司可花钱购买、享有一定财产权益，现实世界的土地法是否适用，现实世界的法律是否适用于入侵元宇宙私人领地的用户，是否可通过虚拟房地产获得抵押、进行融资？〔48〕三是隐私保护问题。如果没有进行适当的安全保护，分布式数字账本和数字钱包中的 NFT 信息可能会被公开访问，其中涉及的个人可识别信息会被其他用户看到。与垃圾邮件类似，用户可能会收到并不想要或非法的 NFT，比如包含网络淫秽内容的 NFT，因为有些交易是不需要接收者同意的。〔49〕四是金融安全问题。近期炒作 NFT 的现象显示，NFT 具有金融属性，可能受到证券、银行、货币等金融法律法规监管，尤其是 NFT 项目涉及利用分布式自治组织（decentralized autonomous organization，DAO）集资投资、分利润

〔42〕 参见前引〔28〕，陈吉栋文。

〔43〕 See LCX AG v. John Doe Nos. 1－25，Index No. 154644/2022 (N. Y. Supreme，Ct.，2022).

〔44〕 See Lavinia Deborah Osbourne v. (1) Persons Unknown (2) Ozone Networks Inc. trading as Opensea，available at https://www.signaturelitigation.com/nfts-recognised-as-property-lavinia-deborah-osbourne-v-1-persons-unknown-2-ozone-networks-inc-trading-as-opensea/，last visited on May. 28，2022.

〔45〕 See Shaun Leong，Withers Obtains Worldwide Injunction for Singaporean to Freeze Sale of Rare Bored Ape Yacht Club NFT，Withers Khattar Wong (May 18，2022)，available at https://www.withersworldwide.com/en-gb/insight/withers-obtains-asia-s-first-nft-freezing-injunction，last visited on Jul. 5，2022.

〔46〕 参见曲忠芳、李正豪：《“NFT 侵权第一案”镜鉴：元宇宙平台担责 三大安全风险待解》，载《中国经营报》2022 年 5 月 9 日，第 21 版。

〔47〕 See Sophie Goossens & Nick Breen，Ownership in the metaverse-the great illusion of NFTs，in Reed Smith，Guide to the Metaverse，2021，pp. 55－58.

〔48〕 参见前引〔13〕，Jerameel Kevins 文。

〔49〕 参见前引〔39〕，美国政府问责局文。

的情况。〔50〕2022 年 4 月 13 日，中国互联网金融协会等三协会发布《关于防范 NFT 相关金融风险的倡议》指出，NFT 作为一项区块链技术创新应用，存在炒作、洗钱、非法金融活动等风险隐患。2022 年 5 月 19 日，由新华社主办的《半月谈》官方公众号发布题为《别让“NFT”成炒作新宠》的文章，对国内 NFT 行业存在的金融化倾向、炒作倾向及产品竞争同质化等问题进行点评，认为一些数字藏品被拆分交易，打破了 NFT 的非同质化特性，可能促使 NFT 相关业务演变成非法集资、非法发行证券等非法、金融活动。同时，国内 NFT 发行方和交易平台尚未被强制要求对发行、售卖、购买主体进行实名认证，为 NFT 领域洗钱问题埋下隐患。〔51〕五是税收问题。在购买和出售 NFT 资产时，是否需要缴纳相关的所得税和销售税？例如，印度税务部门将于 2022 年 7 月 1 日起对虚拟数字资产（VDA）征税，包括加密货币和非同质化代币（NFT）。

三、元宇宙的法律规制建议

元宇宙治理问题是影响元宇宙发展的一个关键因素。从元宇宙整个行业来看，治理决定了未来元宇宙的行业格局。元宇宙相关的监管规则不仅复杂，而且已经成为摆在我们面前的现实问题。〔52〕基于元宇宙的构造，程金华教授认为元宇宙的基本治理逻辑在于：现实世界为元宇宙发展提供法治、现实世界与元宇宙交互时进行共治以及元宇宙内部生态系统建设和运行的自治。〔53〕结合上述元宇宙的法律问题，笔者进一步阐释认为，元宇宙的法律规制主要有三个层次：首先，现实世界的法律法规基本都能适用于元宇宙空间，是一种映射直接适用；其次，针对元宇宙放大而复杂化特定领域的法律问题，需要对现实世界法律法规做相应修改完善后，再进行延展适用；最后，就元宇宙特殊问题，有待制定新的规则，进行专门立法规制。

（一）映射直接适用

元宇宙并非“法外之地”。历史证明现实世界的政府完全有能力控制线上活动。3D 空间并没有什么独一无二的地方需要我们采取全然不同的监管路径，适用于网络空间的法律规则能够直接或间接地适用于元宇宙。〔54〕现实世界的法律是元宇宙治理的主要规则形式，这是毫无疑问的。毕竟，现实世界才是元宇宙的“母体”，而不是相反。〔55〕因此，现实世界的法律规则，基本都能同样映射延展适用于元宇宙空间。例如，欧洲议会强调，隐私和数据保护框架确实适用于元宇宙，其呼吁欧盟委员会确保在元宇宙中的公司和实体遵守现有法律框架。〔56〕再如，元宇宙空间里，发生的名誉权、名称权、姓名权、肖像权等民事侵权甚至是刑事犯罪行为，都能将现实世界

〔50〕 参见前引〔15〕，Jon M. Garon 文。

〔51〕 参见兰天鸣：《别让“NFT”成为炒作新宠》，载 http://m.banyuetan.org/jrt/detail/20220523/1000200033134991653012333494625312_1.html，最后访问时间：2022 年 6 月 8 日。

〔52〕 参见张晓添：《元宇宙有五大长期价值，大型互联网公司具备天然优势——对话德勤管理咨询中国元宇宙卓越中心领导合伙人王嘉华》，载《证券市场红周刊》2022 年第 20 期。

〔53〕 参见程金华：《元宇宙治理的法治原则》，载《东方法学》2022 年第 2 期。

〔54〕 See Andrés Guadamuz, Back to the Future: Regulation of Virtual Worlds, 4 SCRIPTed 242 (2007).

〔55〕 参见前引〔53〕，程金华文。

〔56〕 参见前引〔17〕，European Parliamentary Research Service 文。

的法律法规直接予以适用。

（二）延展修正适用

首先，完善制定元宇宙隐私和个人信息保护的特别条款。基于元宇宙具有的一些独特性质，当前一些个人信息保护规则可能并不能直接适用于元宇宙。据此，有人呼吁修订和更新欧盟《一般数据保护条例》（GDPR），GDPR 对由元宇宙带来的一些挑战和复杂性问题未作出相关规定，例如需要监管在无意识行为中收集的数据，或者与人工智能互动产生的数据。〔57〕因此，有必要修订完善现有个人信息保护规则，延展制定元宇宙隐私个人信息保护的特别条款，应强调隐私保护的基本原则，充分利用数据混淆（data obfuscation）、加密和聚合（aggregation）等数据技术，注意个人数据的存储，并探索契合元宇宙的个人数据使用规则。〔58〕

其次，完善网络数据安全配套法规。2015 年《国家安全法》对“数据的安全可控”作出原则性规定，2021 年颁行的《数据安全法》作为我国数据领域的基础性法律，确立了数据分类分级管理、数据安全审查、数据安全风险评估、监测预警和应急处置等基本制度。国家网信办发布的《互联网信息服务算法推荐管理规定》《网络音视频信息服务管理规定》《网络信息内容生态治理规定》《区块链信息服务管理规定》等规定，涉及元宇宙相关的算法推荐、内容治理、深度合成和数据出境等内容，初步建立起相关的监管规则。但是，在元宇宙内兼顾隐私保护和数据合规利用，系统至少应满足数据的全生命周期安全可信、用户自主控制数据、支持各方进行分布式协同治理这三个基本要求，元宇宙场景下数据都存储在用户自己或者受委托信任的节点上，各个节点构成一个“分布式自组织”（DAO）。〔59〕因此，有待进一步完善网络数据安全相关配套法规，加快制定多层次的数据安全相关技术标准规范，对元宇宙场景下数据的全生命周期安全可信、数据可携带自主可控、DAO 数据安全、内容治理、数据跨境等方面进行有效法律规制。

最后，修正形成新的知识产权授权和权益分配机制。虚拟世界中的创造大多具有衍生属性，虚拟创作者不太可能享有强的知识产权保护，因此，在版权法适用于虚拟世界之前，必须进行修订。版权法不适应虚拟世界中常见的合作型原创，很难将这种原创方式放进版权法的传统定义之中，只有改革规则才能促进有意义的分析。在版权法适用于虚拟世界的前提下，扩大合理使用在虚拟世界中的适用范围、推行虚拟衍生作品的强制许可将促进创新，更有效地实现版权法的目标。〔60〕总之，需要修正完善现有知识产权法律，顺应用户生成内容（UGC）方式的发展，形成新的知识产权授权和权益分配机制。

（三）专门立法规制

其一，构建统一的分层次的数字身份体系。身份认证成为用户访问元宇宙的“护照”。身份是 NFT 的基础，借由数字身份的建构，加之 NFT 作为流通工具，用户能够在虚拟空间与现实社会之间保持高度同步和互通。〔61〕数字身份被广泛认为是下一代身份认证手段系统，很多国家和

〔57〕 参见前引〔17〕，European Parliamentary Research Service 文。

〔58〕 See Rocio de la Cruz, Privacy Laws in the Blockchain Environment, SSRN (Mar. 19, 2020), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3543901, last visited on Jun. 30, 2022.

〔59〕 参见徐磊、赵扬：《元宇宙的隐私保护：技术与监管》，中金研究院研究报告，2022 年 6 月 20 日。

〔60〕 参见前引〔21〕，Matthew R. Farley 文，第 1－32 页。

〔61〕 参见前引〔28〕，陈吉栋文。

地区都已经陆续通过公共部门或私有部门采取行动来应对数字身份问题。例如美国积极实施可信数字身份战略，数字身份立法呈现出系统化趋势，并已在技术标准规范层面形成系统化指南，建立数字身份标准框架，美国商务部下属国家标准与技术研究院（NIST）发布经修订的第三版《数字身份指南》（Digital Identity Guidelines），美国比尔·弗斯特（Bill Foster）等议员提出了《2020年改善数字身份法案》和《2021年改善数字身份法案》。欧盟层面，欧洲议会和理事会2014年发布的《内部市场用于电子交易的电子识别（eID）和信任服务条例》（第910/2014号条例）是欧盟第一个数字身份立法，旨在为跨境电子识别、验证和网站认证提供基础。在第910/2014号条例的基础上，2021年6月，欧盟委员会发布《欧盟议会和欧盟理事会修订欧盟第910/2014号条例、建立欧盟数字身份框架的提议》，提出建立一个值得信赖、安全的数字身份框架，敦促成员国为公民设立数字身份档案系统。2020年3月，G7反洗钱金融行动特别工作组（Financial Action Task Force）发布《数字身份监管指引》（Digital identity Guidance），适用对象主要是政府、金融机构、虚拟资产服务提供商和其他受监管实体，主要规范因数字身份引起的洗钱风险。2022年3月，英国政府宣布启动数字身份立法，设立一个新的数字身份和属性办公室，旨在建立稳健安全的认可和认证流程和信任标识，确认数字形式的身份的有效性等同于实体形式的身份（如实体护照）。2018年9月11日，泰国通过《数字身份验证法案》（The Proofing and Authentication of Digital Identity Bill），旨在为成立数字身份验证监督管理委员会做准备，以落实提高泰国数字身份验证水平，并使之能够全面通过数字渠道进行的计划。

我国也出台了《居民身份证法》《反洗钱法》《网络安全法》《个人信息保护法》及其配套法规、技术标准等相关法律法规，规范真实身份认证等问题，但是还主要是单一应用账户模式，尚缺乏对更高阶段的联盟式和分布式数字身份模式的法律回应，更缺乏统一和专门的身份认证管理法律法规。从国外经验和相关行业实践来看，建议从以下三个层面构建我国可信数字身份法律体系：一是推动出台数字身份国家战略，构建一套包括专门立法、基础设施建设、技术标准规范和行业最佳实践等在内的数字身份战略体系。二是通过数字身份专门立法，建立统一的分层次的数字身份体系。数字身份体系包括身份层、验证层、应用层和数据层四个层次，身份层又可分为法定身份（基础身份）和商业身份（应用身份）。明确规定基于用户个人身份证号码建立起国家法定的、唯一的、权威的用户数字身份体系，商业机构等其他主体基于统一的法定的基础数字身份凭证，构建可信的商业数字身份，并基于基础身份凭证，实现可信数字身份在多个生态圈中的互联互通，打通法定身份和商业身份的互联互通，推动商业领域数字身份的跨平台登陆和互操作。三是推动国家数字身份基础设施建设，积极推进数字身份新技术研究，制定数字身份技术标准规范（国家标准、行业标准、团体标准、企业标准等），推动数字身份基本服务和商业模式创新的落地。

其二，建立数据资产确权利用规则。数据新型财产权从体系上说，应该在区分个人信息和数据资产的基础上，进行两个阶段的权利建构：首先，对于用户，应在个人信息或者说初始数据的层面，同时配置人格权益和财产权益；其次，对于数据经营者（企业），在数据资产化背景下，基于数据经营和利益驱动的机制需求，应分别配置数据经营权和数据资产权。〔62〕如前文所述，

〔62〕参见前引〔36〕，龙卫球文。

基于数字身份及其身份行为，产生了大量各类的个人数据，应对其进行定价和确权，通过法定基础身份和商业应用身份的互联互通，将分散各处、各种数字服务提供者自行管理的身份信息进行连接和交互，积累汇聚于用户跨平台的个人数据账户，经用户授权后，其他机构或平台可以访问和应用相关数据，在不调走数据的基础上经过安全、协同计算，实现数据账户的跨机构共享使用，为用户量身定做如金融产品等各类数字增值服务产品。通过包括本人数据管理模式（my data）在内的方式，让消费者可以去获取和携带自己的消费数据，促进数据的分享、流通利用。个人基础数据的占有权、使用权、获益权都可以在授权访问数据时，通过与数据需求方签订相应的合同来解决。

同时，平台对用户在其应用上产生的各类数据提供记录、检索、整理、挖掘、加工和处理等增值服务，经过匿名化脱敏处理后，产生各类数据服务产品，可以与第三方共享，甚至进行数据交易。因此，应当允许数据处理者享有经个人数据主体同意基于基础数据进行加工编辑分析而产生的增值数据所有权。〔63〕通过数据资产相关立法和统一的基础数据技术标准规范，建立数据产权制度，完善数据资产确权、利益分配机制和流通利用规则，激发个人数据中的资产基因，促进各类数据更便捷地流通利用。

其三，建立统一的 NFT 监管框架。针对前文所述的 NFT 挑战问题，在美国，2022 年 3 月，美国总统拜登签署《关于确保负责任地发展数字资产》的 14067 号行政命令（Executive Order on Ensuring Responsible Development of Digital Assets），详解美国数字资产监管行动框架，旨在解决数字资产及其底层技术的潜在风险。2022 年 3 月，司法部审理了一起利用 NFT 进行投资诈骗的案件。2022 年 4 月，全球税务执法主席联盟发布了如何识别利用 NFT 进行洗钱和其他非法用途的公告。但美国没有针对性的规制 NFT，NFT 在美国法下的法律地位和监管分类尚不明确，其取决于 NFT 的特征及销售方式，NFT 可能落入证券、反洗钱、制裁等监管框架内。目前美国已出现主张 NFT 构成投资合同、进而应受证券法管辖的案例。〔64〕2022 年 6 月 7 日，美国参议院农业委员会成员柯尔斯滕·吉利布兰德（Kirsten Gillibrand）和参议院银行委员会成员辛西娅·卢未斯（Cynthia Lummis）提出了《金融创新责任法案》（Responsible Financial Innovation Act），旨在为数字资产创建一个完整的监管框架，鼓励负责任的金融创新、灵活性、透明度和消费者保护，同时将数字资产纳入现有法律，提高不断增长的数字资产和区块链行业的确定性和清晰度。〔65〕

欧盟也没有专门针对 NFT 出台具体法规，但 NFT 发行的特征可能触发证券领域加密资产市场法规等法规。2020 年《加密资产市场条例（草案）》可能规制 NFT 相关的一部分市场活动；NFT 可能落入欧盟反洗钱指令的规制范围中，欧洲议会成员在 2022 年 7 月 5 日公布的拟议修正案中表示，NFT 交易平台应遵守欧盟反洗钱（AML）法律，因此，市场经营者需要就 NFT 销

〔63〕 参见前引〔34〕，丁道勤文。

〔64〕 See Friel v. Dapper Labs，Inc. et al.，No. 1：21-cv-05837（S. D. N. Y.）.

〔65〕 See Lummis，Gillibrand Introduce Landmark Legislation to Create Regulatory Framework for Digital Assets，avalilable at https://www.lummis.senate.gov/press-releases/lummis-gillibrand-introduce-landmark-legislation-to-create-regulatory-framework-for-digital-assets/，last visited on Jun. 19，2022.

售进行反洗钱合规。英国没有针对性的规制 NFT，其可能落入特定加密资产的范围，进而受到监管。在个案中将根据 NFT 的结构、性质（是否具有电子货币或证券代币的特征）来判断 NFT 的分类及是否属于现有监管范围。新加坡没有针对性监管 NFT，监管一般考察代币的标签和特征，如果 NFT 是受到监管的，那么就需要遵守合规要求。2022 年 5 月 13 日，新加坡最高法院有史以来第一次发布了禁止出售 NFT 的禁令，法院承认 NFT 是有价值、需要承认、可以保护的财产。5 月 27 日，新加坡中央公积金局（CPFB）建议将 NFT 作为多元化投资组合的一部分，代币同行分为安全代币、支付代币和使用代币，对应不同的监管框架。在德国，NFT 可以被用于投资，可能构成《德国银行法案》项下的加密资产。NFT 也可能构成《德国资本投资法案》项下的投资产品。在意大利，NFT 可能构成“虚拟货币”，落入欧盟《反洗钱指令》的范围，触发反洗钱义务。一些 NFT 也可能构成投资产品，受《意大利合并金融法案》监管，需要得到额外的许可。在日本，NFT 不是代币，不具有结算功能，因此不会被作为加密资产进行监管。大部分 NFT 不受任何监管，卡片或游戏内物品的 NFT 交易现在在日本非常普遍。若在游戏内发行 NFT，可能触发《反不合理溢价及误导性说明条例》和刑法典中的赌博条款。日本加密货币商业协会出台了 NFT 指南。〔66〕

在中国，虽然对于 NFT 没有统一的监管框架，但金融监管部门发布并实施了一些限制性政策，严格限制加密货币和加密资产活动。2012 年 7 月，《国务院办公厅关于清理整顿各类交易场所的实施意见》明确要求，交易场所及其分支机构不得将任何权益拆分为均等份额公开发行。中国互联网金融协会等三协会发布《关于防范 NFT 相关金融风险的倡议》，强调 NFT 去金融化，要求“不在 NFT 底层商品中包含证券、保险、信贷、贵金属等金融资产，变相发行交易金融产品”。2022 年 6 月 10 日，福建省地方金融监督管理局披露《福建省清理整顿各类交易场所工作小组关于防范 NFT 违规风险的提示函》，明确要求“福建省交易场所不得开展 NFT 交易相关活动”。

为了维护好元宇宙内的经济体系，防止不法分子通过元宇宙内的经济体系进行洗钱、诈骗等违法活动是需要解决的重点难题之一，因此，建议从国家层面建立起统一的 NFT 监管框架，严格监管加密货币和加密资产市场。现阶段，坚持“去金融化”理念，监管重点聚焦平台，要明确 NFT 交易的多方法律关系，压实主体责任。〔67〕解决好 NFT 的权属、金融风险、个人隐私信息保护等问题，才能让 NFT 这一区块链技术创新应用，持续健康丰富数字经济模式、促进文创产业大发展。

四、结　语

互联网信息技术发展“一日千里”，元宇宙技术和应用仍在不断迭代创新，在未来很长的一段时间里，仍将处于弱元宇宙阶段。在向强元宇宙阶段发展的进程中，未知远大于已知，元宇宙

〔66〕 See Diego Ballon Ossio & James Cranston et al., *Non-Fungible Tokens: The Global Legal Impact*, Clifford Chance, 2021, pp. 2 - 13.

〔67〕 参见程啸、王苑：《透视“元宇宙侵权第一案”数字艺术品法律风险如何规制》，载《光明日报》2022 年 6 月 11 日，第 5 版。

将持续放大和复杂化一些法律问题，同时元宇宙的特殊性法律问题也在不断变化中。不宜高估和热炒元宇宙概念，也不应过度放大甚至妖魔化元宇宙的各种问题。元宇宙并非“法外之地”，现实世界相关法律法规基本都能直接映射适用于元宇宙空间，这是元宇宙法律规制的基本原则。针对那些放大而复杂化特定领域的法律问题，相关法律法规需要做相应修改完善后再进行延展适用，而就元宇宙带来的特殊问题，有待制定新的规则，进行专门规制。

Abstract：The metaverse is a digital ecosystem in which the real and virtual world blend and coexist through digital technologies such as virtual reality or augmented reality. A number of legal issues in the real world will likely be amplified and become more complicated in the metaverse. For example, protection of user privacy and personal information may be challenged as the metaverse involves comprehensive collection of personal sensitive information in a constant and involuntary manner. Data security systems could be greatly impacted by real-time interactive processing of massive data and the widespread application of encryption network technology. The model of user generated content (UGC) may pose new challenges to the right confirmation of content and the distribution mechanism of benefits with regard to intellectual property rights. Competition concerns may arise when users are free to login in with one account across all platforms with interoperability realized. Other unique issues concerning the metaverse include a lack of unified and credible system of digital identity, uncertainty in the rules governing right confirmation and use of data assets, and prominent financial risks associated with NFT. Therefore, to regulate the metaverse and address legal issues concerned, the following principles should be observed. Firstly, the existing legal framework in the real world can directly apply to the metaverse. Secondly, the existing rules with respect to protection of personal information and cybersecurity, data security, as well as intellectual property, may be subject to revision and improvement. Thirdly, new rules could be formulated, such as special provisions governing user privacy and protection of personal information in the metaverse, trusted norms on full-lifecycle data security, and new intellectual property authorization rules for the UGC. In conclusion, this article proposes to develop national strategies for digital identity, establish a unified and hierarchical system of digital identity by introducing specific legislation, formulate new legal rules for the right confirmation and use of data assets, and build a unified regulatory framework for NFT at the state level.

Key Words：metaverse, digital identities, data assets, non-fungible tokens (NFTs)

（责任编辑：刘　权　赵建蕊）

财经法学 No. 5，2022
pp. 35 - 53

元宇宙金融规制理论

邓建鹏*

内容提要：元宇宙金融以基于公共区块链的去中心化金融为核心。这种新型金融开创了低成本、高效率的运营方式，但因其无准入门槛，全球参与主体身份不明确、防篡改、抗审查、自我创制规则及自动运行等特点，冲击着金融监管法律体系。然而，元宇宙金融并非绝对不可规制，其历经“去中心化”到“再中心化”的演进，监管机构以“再中心化”的主体为重要抓手，通过非正式指引，出台区块链技术与代码安全的国家标准及正式法规、推动传统金融和元宇宙金融融合等方式，影响基于代码的规则体系、提升金融安全与形塑社区自治规范。不过，元宇宙金融“再去中心化”的演变决定了其在较长时期不能完全被法律规制。

关键词：元宇宙金融　区块链　再中心化

一、导　论

（一）被忽视的核心内容

元宇宙（metaverse）概念起源于尼尔·斯蒂芬森的科幻小说《雪崩》（Snow Crash）。作为3D数字化虚拟共享空间，元宇宙以高速通信网络为基础，支持虚拟时空的大量应用创新，以高性能的虚拟现实（VR）或增强现实（AR）等技术设备及软件带给用户高沉浸、低延迟、多样性和即时参与的感受，借助人工智能驱动的虚拟数字人将元宇宙的内容有组织地呈现给用户。2021年下半年以来，元宇宙概念在学术界被万众瞩目，相关论文如过江之鲫。这些研究主要从传播、文化或哲学思考等领域入手。比如《探索与争鸣》等杂志于2022年2月主办“认识元宇宙：文化、社会与人类的未来”论坛，与会学者就“元宇宙”的哲学基础、道德伦理、媒介实践、社会

* 邓建鹏，中央财经大学法学院教授。
本文为中央财经大学新兴交叉学科建设项目“金融系统安全与区块链监管科技”（批准时间：2021—03）阶段性成果。

特征、主体特征等方面开展交流和反思。〔1〕其他一些核心期刊发表的“元宇宙”论文亦着重从社会传播、哲学思考或政治风险角度切入。〔2〕法学“元宇宙”主题论文有的从宏观或抽象层面论述，〔3〕有的则尝试分析其铸币权等细分问题。〔4〕

然而，元宇宙最引人注目的莫过于数字创造等经济活动。有学者认为元宇宙能够提供各种数字产品和服务，其成败取决于其能否具有实质性的丰富活动，使人们接入元宇宙是一件既具有经济价值又具有学习、社会、娱乐等价值的活动。〔5〕业界专业人士把数字资产创造、交换、消费等所有在元宇宙进行的经济活动统称为元宇宙经济。数字经济是以数字要素作为关键生产资料的经济活动，传统经济升级的方向是数字经济，元宇宙经济是数字经济的一个子集，是其最活跃、最彻底、最具革命性的部分。〔6〕元宇宙经济要素规模无限大，消费频率大幅提高，边际成本趋零化，因此元宇宙经济规模将是现实世界的数倍。〔7〕这样一种由实际生产和消费支撑的高效虚拟经济系统将超越现实世界大多数传统经济体的规模。〔8〕

2022 年 3 月，花旗银行的“全球视野与解决方案”部门（Global Perspectives & Solutions，GPS）发布长达 184 页的深度报告《元宇宙与货币：解密未来》，该报告指出：“到 2030 年，元宇宙经济潜在市场规模将达 8 万亿美元到 13 万亿美元之间，潜在用户将高达 50 亿户。”报告着重指出：“随着元宇宙发展，将需要一系列金融服务支持其活动。元宇宙金融（MetaFi）融合了当今两大技术趋势：元宇宙和去中心化金融（DeFi），即‘元宇宙的去中心化金融工具’，将推动去中心化金融快速增长。从最初的资本形成到支持元宇宙内的商业，金融服务可以在其演变中发挥重要作用。”〔9〕该报告是笔者迄今所见元宇宙领域最详细、最专业的研究。

根据底层技术架构和治理权力的特征，元宇宙分为封闭式（中心化）与开放式（去中心化）两种结构。〔10〕封闭式元宇宙由特定法律主体（公司或个人）掌控，如美国 Epic 公司旗下游戏《堡垒之夜》（Fortnite）及元宇宙上市第一股“罗布乐思”（Roblox）等，其借助相对封闭、分割的特征，由所属公司获取大部分收入与利润。以“罗布乐思”为例，首先，其允许用户以平台自主发行

〔1〕 参见屠毅力、张蕾等：《认识元宇宙：文化、社会与人类的未来》，载《探索与争鸣》2022 年第 4 期。

〔2〕 参见喻国明、耿晓梦：《何以“元宇宙”：媒介化社会的未来生态图景》，《新疆师范大学学报（哲学社会科学版）》2022 年第 3 期，等等。

〔3〕 参见程金华：《元宇宙治理的法治原则》，载《东方法学》2022 年第 2 期；张钦昱：《元宇宙的规则之治》，载《东方法学》2022 年第 2 期。

〔4〕 参见袁曾：《元宇宙空间铸币权论》，载《东方法学》2022 年第 2 期。在国外，个别学者分析元宇宙化身（虚拟人）的法律问题。See B. C. Cheong, Avatars in the Metaverse: Potential Legal Issues and Remedies, International Cybersecurity Law Review (2022), available at https://link.springer.com/article/10.1365/s43439-022-00056-9#citeas, last visited on Aug. 8, 2022.

〔5〕 参见何哲：《元宇宙新经济的裂变及可能趋势》，载《人民论坛》2022 年第 7 期。

〔6〕 参见赵国栋、易欢欢、徐远重：《元宇宙》，中译出版社 2021 年版，第 30、86-87 页。

〔7〕 参见邢杰、赵国栋等：《元宇宙通证》，中译出版社 2021 年版，第 32 页。

〔8〕 参见长铗、刘秋杉：《元宇宙》，中信出版社 2022 年版，第 58 页。

〔9〕 See Metaverse and Money: Decrypting the Future, available at https://www.citivelocity.com/citigps/metaverse-and-money/, last visited on May 22, 2022.

〔10〕 有学者将元宇宙分为中心化元宇宙和去中心化元宇宙。参见王德夫：《论“去中心化元宇宙”的风险识别与法律治理——以“元宇宙使馆”事件为观察》，载《荆楚法学》2022 年第 3 期。但极少有法学研究者指出这一重大区分并作差异化研究。在前区块链时代，少量开创性研究停留于对中心化元宇宙的论述。See Cory Ondrejka, Escaping the Gilded Cage: User Created Content and Building the Metaverse, 49 *New York Law School Law Review* 81 (2004).

的虚拟货币“罗布币”（Robux）购买平台内用户生成内容（user generated content，UGC）或平台增值服务；其次，用户只能按平台设定价格向平台以美元购买罗布币，并限于平台内使用；最后，“罗布乐思”允许开发者通过开发者交换计划（DevEx）将赚取的罗布币兑换成法定货币。

开放式元宇宙并无特定法律主体掌控，如部署在以太坊等区块链的 The Sandbox 或 Decentraland 等。开放式元宇宙被认为是下一代互联网，即 Web3.0，由区块链、智能合约与非同质化通证（NFT）等构成。〔11〕这种元宇宙主要由用户构建并拥有，用户生成内容，允许内容创建者控制其内容，享有数字作品的权利。与 Web2.0 时代超级平台垄断用户数据和大部分收益不同，Web3.0 是用户和建设者共同拥有网络与数据，这在区块链技术条件下方能实现。开放式元宇宙是“利益相关者机制”，逐渐形成用户和建设者自治的组织形式（DAO），组织规则由程序代码执行，建设和维护元宇宙的社区成员分享利益，共有和共治虚拟空间，这需要应用区块链的共识机制及数字通证作为经济激励机制。综上，开放式元宇宙将与区块链深度融合，释放用户数字创造动力，代表未来的行业发展方向。

区块链为元宇宙金融提供必要基础架构、NFT（非同质化通证）和数字通证（以太币等同质化通证），为数字创造实现价值标识（确权）与价值转移（交易）。2004 年，学者指出自由市场与财产权利的界定是创新的先决条件。元宇宙要取得成功，则要求虚拟财产必须能够转换成现实世界的财产。这个自由市场要求创造者对财产拥有相应权利，方有创造财富的动力，以促进增长。〔12〕但在前区块链时代，个人拥有数字作品的财产权利缺乏技术支持，多停留于设想中。与封闭式元宇宙由所属公司掌控数字资产所有权（如游戏平台控制各类游戏道具与装备）不同，开放式元宇宙需要独立于特定应用项目的数字资产所有权，以太坊等技术标准允许元宇宙用户以可控方式拥有数字资产。用户拥有数字资产的所有权，开辟资产金融化的途径——质押、借贷、交易和衍生品等，这些业务在去中心化金融应用中已比较成熟，构成元宇宙金融主要内涵。

区块链原生数字通证或私人加密货币是激励手段，也可能成为价值储藏的载体，与稳定币构成元宇宙的支付工具。〔13〕去中心化金融降低了人们进入金融的门槛，为人们通过加密资产获利创造机会。〔14〕在这个开放系统上创建钱包、转账与交易均无需提供个人身份等关键信息，应用无需许可，无需中介机构（如券商、银行或第三方支付机构），所有业务通过区块链智能合约自动执行；无需昂贵办公场所和庞大合规团队，交易费用低于传统金融机构；各类应用程序像“金钱乐高积木”一样搭建与分工协作，允许用户创建、修改、混合、匹配或链接任何现有的去中心化金融产品；智能合约应用程序相互叠加，生成可互操作和组合的金融业务。去中心化金融的一些理念富有积极意义，如消除中间环节的暗箱操作，降低中介风险，个人掌控加密资产，交易记

〔11〕 See Paul P. Momtaz，Some Very Simple Economics of Web3 and the Metaverse”（April 17，2022），available at SSRN：https://ssrn.com/abstract=4085937，last visited on Jun.1，2022.

〔12〕 参见前引〔10〕，Cory Ondrejka 文，第 100－101 页。

〔13〕 稳定币通常与美元一比一挂钩，近年成为加密资产交易的主流支付工具，其功能与风险，参见邓建鹏、张夏明：《稳定币的内涵、风险与监管应对》，载《陕西师范大学学报（哲学社会科学版）》2021 年第 5 期；邓建鹏、张夏明：《稳定币 USDT 的风险及其规制对策》，载《经济社会体制比较》2021 年第 6 期；Douglas Arner，Raphael Auer & Jon Frost，Stablecoins：Risks，Potential and Regulation，BIS Working Papers No 905，November 2020.

〔14〕 本文探讨的加密资产是区块链上发行的虚拟货币/私人加密货币/数字通证，如比特币、以太币和稳定币等同质化通证（FT）及非同质化通证（NFT），加密资产是数字资产的一个子集。

· 37 ·

录公开透明，受公众监督等。在元宇宙中，可组合性和互操作性使不同加密资产能够应用去中心化金融协议进行传输和交换。用户在去中心化的交易所兑换不同私人加密货币，将私人加密货币存入借贷协议赚取收益，或用“跨链桥”将私人加密货币转入其他区块链系统，这些特征与元宇宙金融业态融合。

（二）法学研究的偏差

元宇宙金融以分布式自治机制（DAO）和数字通证（token）作为组织模式和激励方式，分布式自治机制建立在区块链和智能合约基础上，数字通证是激励参与者完成交易的驱动机制。元宇宙金融是以区块链技术、智能合约和分布式自治机制等为基础的第三代互联网在金融领域的重组。近年去中心化金融应用主要有三种：一是借贷，用户可基于以太坊的借贷协议（如 compound）在其借贷池中存入资产，赚取利息，或利用该协议质押加密资产以借出稳定币。如质押资产市值下跌或到期用户还款困难，协议将执行清算程序，拍卖质押品以避免损失。二是基于去中心化交易所（DEX）的加密资产交易，去中心化交易所（如 Uniswap）允许人们不经审核即在该应用协议上直接交易，允许人们交易新的加密资产。三是衍生品交易，衍生品平台（如 Synthetix）允许用户杠杆交易，或创建模仿传统股票和商品的“合成资产”，作为交易标的。〔15〕

去中心化金融成为元宇宙金融核心，其发展突飞猛进，至 2022 年 6 月 5 日，据 DeFi Pulse 统计，区块链上借贷、交易及衍生品等加密资产锁仓市值达 540 亿美元以上。〔16〕去中心化金融应用由以太坊拓展到其他区块链系统（如 Solana 等），引起业内人士与各国金融监管机构高度关注，诸如美国证券交易委员会（SEC）表态要监管去中心化金融。〔17〕去中心化金融是近年“破坏式”创新的代表，引发了显著法律风险——去中心化金融衍生品的匿名性和去中心化交易，使监管机构收集信息受阻，可能助长洗钱、恐怖融资及网络诈骗等犯罪，增加取证、侦查难度。〔18〕

然而，近年相关法学研究对加密资产法律属性或反洗钱等细分问题的探讨居多，〔19〕整合性研究较为有限。比如，有学者提出区块链金融的智慧型监管及自我规制、行业规制和监管沙箱等；〔20〕或分析去中心化自治组织的法律属性，提出去中心化自治组织适宜界定为有限合伙，发起人承担无限责任，乃普通合伙人，投资者承担有限责任，乃有限合伙人。〔21〕但这些研究忽视了对重要规制对象的深入分析，难以实现预期目的。有学者提出区块链规制的几个层面，即自主

〔15〕 See Matt Hussey, Ki Chong Tran & Jeff Benson, What is DeFi? A 3-minute guide to decentralized finance—Decrypt, available at https://decrypt.co/resources/defi-decentralized-finance-explained-guide-learn, last visited on Dec. 27, 2021. 有学者将去中心化金融应用概括为开放借贷、去中心化交易所、去中心化自治组织、聚合收益理财、稳定币、非同质化通证（NFT）等。参见郑磊：《去中心化金融和数字金融的创新与监管》，载《财经问题研究》2022 年第 4 期。

〔16〕 参见 https://defipulse.com，最后访问时间：2022 年 6 月 5 日。

〔17〕 See Scott Chipolina, SEC Chair Gary Gensler Wants To Regulate DeFi—Decrypt, available at https://decrypt.co/78933/sec-chair-gary-gensler-wants-to-regulate-defi, last visited on Dec. 27, 2021.

〔18〕 研究者系统指出，去中心化金融存在高杠杆、抵押品不足、无反洗钱机制、无用户身份识别、交易匿名与市场操纵等风险。See Sirio Aramonte, Wenqian Huang & Andreas Schrimpf, DeFi Risks and the Decentralization Illusion, *BIS Quarterly Review*, 32 (2021).

〔19〕 比如，杨延超：《论数字货币的法律属性》，载《中国社会科学》2020 年第 1 期。

〔20〕 参见朱娟：《我国区块链金融的法律规制——基于智慧监管的视角》，载《法学》2018 年第 11 期。

〔21〕 参见郭少飞：《“去中心化自治组织”的法律性质探析》，载《社会科学》2020 年第 3 期。

• 38 •

规制、多方利益相关者共同规制、基于代码的规制等，〔22〕论述多为宏观抽象视野，具体在去中心化金融领域，这些方式的可行性有待观察。有学者认为区块链金融需要在沙箱式监管下实现创新，由监管部门主导完成风险的跟踪测试，金融监管的必要性决定了完全去中心化的公有链不宜适用于金融领域，该领域应淡化“去中心化”，强调分布式、弱中心特征。〔23〕这种应然层面的探索无法回应实然层面去中心化金融及元宇宙蓬勃发展所引发的现实问题。有学者认为区块链治理中驯化“去中心”是历史必然，〔24〕然而如何驯服“去中心化”尚需深思熟虑。

元宇宙虚实结合，将兼容去中心化金融与中心化金融（传统金融），但中心化金融或传统金融多由特定法人主体控制，承担法律责任的主体明确，在现有金融监管法律框架内基本可得到规制。开放式元宇宙监管环境远未成熟，去中心化金融业态将是元宇宙最具活力、革命性，甚至“破坏力”的部分，但其在现有法律与监管框架内几乎完全空白，引发巨大的规制难题，尚未引起各国监管机构普遍重视。元宇宙与去中心化金融结合带来的风险与挑战，〔25〕亟需法学研究者针对其“去中心化”表象，分析法律风险，重点思考“规制谁、如何规制、规则原则及规则方式可能的局限”等系列理论问题。综上，本文以提升元宇宙金融可规制性（regulability）作为研究核心：首先，分析开放式元宇宙金融的底层技术，即区块链对现行法律构成挑战的原因；其次，讨论元宇宙金融可规制的主要对象；再次，探索规制方式与规制重点阶段；复次，剖析规制局限及原因；最后是结语。

二、“去中心化”与“中心化”的对立

（一）元宇宙金融“去中心化”的法制挑战

元宇宙金融实为区块链去中心化金融的应用，与法律中心化特征之间存在矛盾，这是元宇宙金融挑战法律与监管规则的主因。传统法律关系由权威的中心化机构（如立法、执法和司法机关）确立、宣示和保证执行。诸如各类权益证书由中心化机构（如房产管理部门、车辆管理部门）登记、确权并受法律保护，权利和义务主体的特定化是明确法律关系的前提。参与和运维区块链系统的网络节点分布于全球，交易无需识别用户真实身份，义务承担者分散化或无法确定，权利人的请求权可能失去特定对象。法律体系是中心化社会的产物，去中心化意味着区块链系统缺乏明确法律主体，法律规制缺乏特定对象，为不特定参与者规避法律责任提供便利，甚至导致“法不责众”的局面。

区块链部署去中心化应用为交易者提供未经监管者许可的期权、借贷等各类金融产品与服务。在基于以太坊自动做市（automated market maker，AMM）交易协议的 Uniswap 上交易，不需要做市商、上币费及撮合模式下超大规模的运算资源，为元宇宙和区块链项目融资及加密资

〔22〕 参见〔英〕罗伯特·赫里安：《批判区块链》，王延川、郭明龙译，上海人民出版社 2019 年版，第 54－80 页。

〔23〕 参见崔志伟：《区块链金融：创新、风险及其法律规制》，载《东方法学》2019 年第 3 期。

〔24〕 参见李佳伦：《区块链信任危机及其法律治理》，载《法学评论》2021 年第 3 期。

〔25〕 学者认为去中心化金融风险种类比传统金融多，在智能合约代码安全、治理风险、流动性、操作、信用、监管等方面都存在风险点。参见前引〔15〕，郑磊文。

产价格发现提供便利。Uniswap 基于以太坊协议，允许用户以去中心化和无需许可的方式促进以太币和其他任意加密资产（要遵循以太坊 ERC-20 协议发行）之间自动兑换。如某种代币不在 Uniswap 上，只需复制和粘贴该代币的智能合约地址就可添加。有学者认为 ERC-20 协议是至今以太坊上发行的受认可程度最高、使用最为广泛的加密资产协议，旨在为以太坊上通证合约提供一个特征与接口的共同标准。但其并未考虑监管方面对加密资产发行的要求，或者说是为避免对生成于公有区块链的加密资产监管而诞生的一种通用的、简单的标准化协议。〔26〕任何用户可在 Uniswap 自由存入代币进行兑换，自由提取，〔27〕没有中心化交易所（CEX）进行用户注册、身份验证和充提币限制，智能合约自动运行，无需像中心化交易所那样，必须核实用户身份信息。很多项目开发团队原来只能先向中心化交易所付费（业界称“上币费”），通过中心化交易所严格审核或社区投票后才能上市交易某种加密资产（IEO）。〔28〕

去中心化金融业务近年来飞速发展，据以太坊市场分析平台 Dune Analytics 的数据，即使在 2022 年 6 月 15 日“币圈”熊市期间，以 Uniswap 为代表的去中心化交易所在一周内仍创下了 230 亿美元的交易量。〔29〕多数国家针对中心化交易所设有严格牌照管制和相应法律与监管。然而，这种商业模式不用验证交易者身份，无人审核特定加密资产是否存在代码漏洞，不必验证资金合法性来源。诸如 Uniswap 仅是一段代码，部署于以太坊上。区块链防删改的特性使上述项目一旦启动，创始人亦无法停止其运行。当前尚无有效法律与监管机制应对之。

（二）元宇宙金融自生规则与法制的分立

元宇宙金融多无明确控制主体，责任承担主体模糊化，无用户真实身份或地理位置信息，增加监管与合法性审查难度。如学者所述：“现有法律体制的监管重点，是负责和协调在线活动的各种中心化中介机构，而部署在区块链上的系统，如果主要或完全借助密码法运作，就难以受到现有法律体制的控制和监管。”〔30〕法律规制对象主要是中心化社会特定的、可承担义务的主体，这是法律规制的前提。元宇宙金融破除现实中心主义的过程中创生新机制，以分布式架构与不确定主体随时参与或退出为特点，这个时空的规则由元宇宙金融社区自生秩序演化而来，影响现实社会人的行为及法律机制。

元宇宙金融的规则自我创生，自我发展，以系统自身商业目的为准则，不以现实世界监管机构的意图为内涵。当法律试图工具主义地对待元宇宙，使之更好地服务于监管者意图时，双方不可避免地会产生对立。公共区块链系统假名或匿名及免授权许可的方式，使其无任何准入门槛。如比特币系统创建全球分布式价值传输网络体系，交易者可低成本跨境转移巨额资产。比特币在传统金融账户体系之外实现了价值传输，客观上规避现行法律与监管要求。比特币系统基于代码的规则与金融监管法律体系不一致。私钥是持有人控制比特币的唯一途径，多保存在每个持有者

〔26〕 参见姚前、林华等：《区块链与资产证券化》，中信出版社 2020 年版，第 201 页。

〔27〕 参见 https://www.feixiaohao.com/coindetails/uniswap/，最后访问时间：2021 年 2 月 26 日。

〔28〕 IEO 即“Initial Exchange Offerings”，一个区块链项目除早期私募由机构参与外，之后的公募和上线交易都是基于某交易所（Exchange）完成。该模式的核心是知名交易所用自身信用为项目方背书。

〔29〕 参见 https://dune.com/hagaetc/dex-metrics，最后访问时间：2022 年 6 月 15 日。

〔30〕〔法〕普里马韦拉·德·菲利皮、〔美〕亚伦·赖特：《监管区块链：代码之治》，卫东亮译，中信出版社 2019 年版，“导论”第 XIII 页。

的本地终端，持有者控制存储或转移价值不用借助金融中介机构。这种去中心化的价值管控方式，使司法机构查封、扣押、冻结违法者财产的传统方式难以执行。〔31〕

网络信息管理部门曾指出“区块链作为一项新兴技术，具有不可篡改、匿名性等特性”〔32〕，但其在《区块链信息服务管理规定》第16条却规定：“区块链信息服务提供者应当对违反法律、行政法规规定和服务协议的区块链信息服务使用者，依法依约采取警示、限制功能、关闭账号等处置措施。”诸如在以太坊系统，单方面修改已记录在区块上的信息（包括限制功能、关闭账号等措施）难度极大，因此前述法规要求如缘木求鱼。有学者认为，某些严格遵循去中心化构想的区块链系统在实质上没有能力对系统上的活动开展实质性审查。对此，一个重要的平台责任确定原则是，必须结合履行能力来确定平台义务。这就意味着，对于区块链平台无法履行的行为，不能为其施加义务。〔33〕

由于区块链分布式账本跨越国界，元宇宙金融全球化应用场景产生的风险难以受到单一国家监管规则约束。各国对加密资产及智能合约监管等存在不同态度又催生了规则空白。链上行为跨越不同司法辖区，而各国法律规制意图并不相同。元宇宙金融中的博彩游戏、跨境资产转移或敏感信息上链等行为在特定国家或地区受法律保护，在另外一些国家或地区则是打击对象，不同国家对同一行为的合法性评判存在显著差异。如何处理不同国家或地区的法律冲突，哪些国家或地区的法律能够得到执行？这带来不同国家或地区监管执法与司法难题。元宇宙金融难以同时满足所有国家或地区规制的差异化内涵。

代码规则允许加密资产、稳定币和智能合约在未受监管机构审批的前提下组成丰富多样的金融业务与产品，这些新生业态的法律地位或法律属性在现有法律与监管体系中多不明朗，使元宇宙金融在现有法律框架下呈现高度不确定状态，其代码规则可能背离现实社会金融监管法律体系。受代码规则约束的各类加密资产的功能及法律性质差异甚大，对法律产生不同影响、冲击或挑战。具体而言，有的加密资产是功能性或消耗性的，比特币则在事实上逐渐成为价值存储的载体，日益成为欧美众多传统投资机构的重要投资标的。以太坊发行的以太币更像是一种“加密燃料”（crypto-fuel）形式的激励，支付程序运行所需要的费用。去中心化组织无法律实体，通过代码规则与数字通证界定成员的贡献量，从而分配相应权益。去中心化金融创造金融工具，也创造金融资产。比如MakerDAO系统既创造借贷协议，也创造稳定币DAI及治理代币MKR。治理代币持有者可对协议参数的更改（例如稳定费或最低质押比率等）投票。MKR根据DAI价格波动而创建或销毁，使DAI价格尽可能接近1美元。MKR还用于在MakerDAO系统上支付交易费用，并为持有人提供MakerDAO批准的投票系统内的投票权。

（三）基于代码治理的元宇宙金融

元宇宙金融借助区块链系统，其代码规则客观上排斥现实社会的中心化权威，加剧了元宇宙

〔31〕 参见《最高人民法院关于人民法院民事执行中查封、扣押、冻结财产的规定》（法释〔2004〕15号）。

〔32〕《区块链信息服务管理规定》，载 http://www.cac.gov.cn/2019-01/10/c_1123971138.htm，最后访问时间：2021年6月5日。

〔33〕 参见马永强：《区块链金融的刑法风险与规则之治》，载《重庆大学学报（社会科学版）》，转引自 https://kns-cnki-net.webvpn.cufe.edu.cn/kcms/detail/50.1023.C.20210610.1109.002.html，最后访问时间：2022年8月8日。

金融与金融监管法律体系的紧张关系。元宇宙各类金融应用搭建在公共区块链系统之上，需要遵守底层协议，随着应用普及，世俗社会的权力由立法、执法与司法等中心化机构部分转移到区块链核心技术开发人员手中。程序员编写的代码成为另一种“法律”，形塑加密资产创造、资产转移、融资借贷和资产交易等行为。在区块链系统，代码确立的规则等同于刚性法律，不遵守其架构，无法处理包括支付、交易、“挖矿”（竞争区块链账本信息记录权以获取加密资产奖励）和数字签名等行为。这个刚性规则排斥违背代码协议的行为，元宇宙金融可在现实社会执法机构、仲裁机构或司法机构等第三方缺失情况下运行自如。

元宇宙金融是自由开放体系，现实社会金融产品可上链交易，元宇宙金融也可向传统金融体系反向渗透。前者如以美元储备支撑的稳定币 USDC 在以太坊上发行和流通，后者如区块链应用项目 Mirror Protocol 和 Synthetix 创造特斯拉公司等知名公司股票的复制版本。项目开发者在区块链上创建“镜像”协议，激励交易者套利价格差异和管理代币实际供应量，使合成股票价格与真实股票基本保持一致。这些代币在 Uniswap 等去中心化交易所交易，被设计成无需购买真实股票，就可反映它们所追踪的股票价格。〔34〕但这些合成产品未受监管，也没有在特定国家证券交易所交易。这些代币化股票发行和交易可能违反证券法。阻止“镜像”股票交易，就必须关闭该应用的实施基础，即遍布全球的以太坊网络节点和开源代码，关停所有“矿机”，这存在现实困难。

在元宇宙金融系统，中央银行法、商业银行法、证券法、货币管理法和外汇管制法等法律被代码置换。现实社会的规则在区块链及元宇宙中的价值转移、支付或交易过程中并非必选项。元宇宙金融依托区块链自治组织机制，其社区投票结果而非法院裁决具有决策权威。比如在 2016 年，“DAO 项目”由于智能合约漏洞，约 1.5 亿美元的以太币（当时价格）被黑客攻击，对此，以太坊社区大部分网络节点投票决定同意“硬分叉”，取回被盗以太币，原以太坊最后被分叉为以太坊（ETH，即“新链”）和以太坊经典（ETC，即“旧链”）。〔35〕在这起涉及巨额资产的重大争议中，其决策过程无监管机构、仲裁机构或司法机构介入，完全由以太坊社区投票表决。传统金融创新产品上市须经监管机构审批，产品背后有明确责任主体，面向合格投资者销售。元宇宙金融产品和服务无需审批，交易通过合约自动执行，实现代码治理与社区“私法自治”。智能合约是对双方合意的特别执行程序，也是权利义务的代码化表述，通常排除合同变更、合同条款重新解释与特殊情况下不履行合同等情况。在传统合同法视野下，发生欺诈、胁迫或显失公平等事由时，合同可撤销或可变更。在智能合约中，执行代码发送到所有系统的节点分布式处理，只有多数节点代码同步修订才能更改原智能合约。因此，元宇宙金融实行代码规则的自我治理，社区规范与内部自治取代法律。

三、“去中心化”与“再中心化”之悖论

综上，元宇宙金融“去中心化”冲击与挑战金融监管法律体系。有学者认为，去中心化结构

〔34〕 See Fake Tesla，Apple Stocks Have Started Trading on Blockchains，available at https://medium.com/bloomberg/fake-tesla-apple-stocks-have-started-trading-on-blockchains-ed3addaf99e，last visited on Jul.8，2021.

〔35〕 参见井底望天、武源文等主编：《区块链世界》，中信出版社 2016 年版，第 74－80 页。

由许多不同参与者管理，有效管控需要努力识别许多不同相关行为者，但这些行为者匿名、难以找到或位于国外时，就很难做到这一点。去中心化还带来法律执行问题，当系统被设计成其运行的责任分散到许多不同参与者时，分配责任和惩罚违规行为会变得很困难。〔36〕对此，从捍卫一国金融监管主权、防范金融风险及推动金融创新角度而言，在借鉴固有互联网规制模式的同时，应着重思考规制元宇宙（及区块链）与规制传统互联网存在什么差异，可规制的对象（法律责任承担主体）是谁。

（一）元宇宙与传统互联网规制差异

元宇宙被视作下一代互联网，讨论元宇宙金融或区块链规制问题时，人们易沿用传统互联网（Web2.0）规则的固有思维。对后者，美国宪法与互联网法专家劳伦斯·莱斯格的《代码 2.0：网络空间中的法律》为本领域经典著作。〔37〕但 Web2.0 时代互联网产业最终被法律规制，关键原因是互联网产业均依托中心化商业机构或法人实体。如亚马逊等商业机构总部均位于特定主权国家范围，背后有明确的高管、实际控制人和投资机构。通过以下层次的制约，平台及用户逐渐被严密规制：一是平台实行内部控制规则，对违背平台规则的交易者施以惩治，如交易者被禁用淘宝账号；二是平台规则正当性不断受法律评价和审查，平台规则逐渐与正式法规融合甚至一致；三是公权力机构通过监管执法与司法，将平台间冲突、平台上发生的交易行为置于规制范围内，比如处罚违背反不正当竞争法或反垄断法的平台。

有学者认为，网络平台经营活动主要依靠消费者权益保护法、反垄断法、反不正当竞争法、电子商务法等法律制度从外部加以规范；平台制定的大量规则对其用户的权利义务起到实质影响；法律也有必要回应平台内部的权力关系与民主诉求。〔38〕基于商业模式便利，诸如淘宝或二手书交易中介商“孔夫子网”等平台事先引导交易者实名化，明确交易者收件地址，鼓励交易者对每次买卖行为互相评分。诸如微信支付及支付宝用户实名制则来自商业机构精准营销及遵照金融监管法律体系关于用户识别、反洗钱等已有规则的要求。总之，平台基本实现法律规制，很大程度是商业机构利益驱动与政府监管合力的结果。此如有学者认为，无论是商业利用还是政治控制的需要，都将不断推动那些增强互联网可规制性的技术——身份验证、数据标识和物理定位——被广泛采用。〔39〕

有学者认为，互联网真实权力机制由三个要素构成：账户、数据和评分。商业和政府力量使互联网控制权重新变得集中，互联网出现独特的中心化控制机制，即少数平台通过“账户—数据—评分”机制加强网络治理。〔40〕互联网规制方式为区块链或元宇宙金融的法律规制似乎提供了参考，但鉴于两者中心化信息互联网和去中心化价值互联网的本质差异，元宇宙金融注定无法照搬固有的规制模式。在 Web3.0 时代，区块链架构有全新的设计和调整，通过分布式记账、密码学原理和共识算法等技术集成解决陌生人主体间信任问题，实现价值可编程，新的构建模块打开

〔36〕 参见〔美〕威廉·马格努森：《区块链与大众之治》，高奇琦等译，上海人民出版社 2021 年版，第 230－231 页。

〔37〕 参见〔美〕劳伦斯·莱斯格：《代码 2.0：网络空间中的法律》（第 2 版），李旭、沈伟伟译，清华大学出版社 2018 年版。

〔38〕 参见刘权：《网络平台的公共性及其实现——以电商平台的法律规制为视角》，载《法学研究》2020 年第 2 期。

〔39〕 参见戴昕：《犀利还是无力？——重读〈代码 2.0〉及其法律理论》，载《师大法学》2018 年第 1 辑。

〔40〕 参见胡凌：《超越代码：从赛博空间到物理世界的控制/生产机制》，载《华东政法大学学报》2018 年第 1 期。

· 43 ·

了新型金融业态的大门。其中多数构建超越了劳伦斯·莱斯格代码 2.0 时代的设想。去中心化的元宇宙金融有自身特质，“无须信任”的架构允许不同参与方无须互相信任就能完成复杂金融交易，实现价值转移，传统互联网则需要诸如评分机制来加强网络治理；传统金融业围绕银行账户展开，元宇宙金融借助区块链用公私钥体系取而代之。综此，元宇宙金融的特殊性要求监管者调整其旧有思维。

区块链账户模式各有千秋，但账户均无需绑定用户身份、识别用户真实性或提供用户通讯地址等任何个人信息，这些特征内嵌于元宇宙金融，使传统互联网账户关键要素被区块链消解。通过不对称加密与共识算法等“技术信任”，区块链无需以评分模式让用户增信。有学者认为互联网平台的社会规范是以诸如身份认证、行为追踪和记录评分等核心内容的权力结果为基础，〔41〕这在区块链中均非必备要素。综上，元宇宙金融规范相较于传统网络规范存在显著差异。固有金融监管模式中，金融机构（确定运营主体）、金融账户（确定用户主体）及牌照管理（确定运营主体合法性）是实现监管意图的关键，但这些因素被元宇宙金融逐一化解。

国外专家认为，与互联网一样，法律总是能适应监管、约束和影响区块链技术的发展。毕竟，区块链只不过是一个去中心化网络，这和互联网并无本质不同。区块链系统必须依赖为底层区块链网络提供支持的新型中介机构，而这些机构易受到监管。此外，这些系统必须依赖代码（或体系结构），它们的运作方式最终取决于市场力量，并受制于社会规范。〔42〕这为区块链及元宇宙的规制提供一些启示，但研究者忽略了两者的重大差异，并未提出有效思路。

（二）元宇宙金融的“再中心化”

有效规制元宇宙金融，应明确其技术底层——区块链的“权力架构”，即在区块链系统发挥关键影响力的私权力主体，确定可规制的重要对象（法律责任承担主体），这是元宇宙金融被金融监管法律规则塑造的前提。如前所述，这个关键性问题在近年研究中多被忽略。有学者认为，应完善区块链相关法律法规及配套制度，加大区块链在金融领域应用的治理。〔43〕然而，法律并非万能，技术总在变异，过度宽泛的建议与有效规制区块链（及元宇宙）存在遥远距离。为常人忽略的是，元宇宙金融虽借助区块链“去中心化”，同时却在若隐若现地“再中心化”。个别研究者断言，“完全去中心化”是种幻觉，去中心化金融平台有一群利益相关者，他们执行决策、实施经营或拥有所有者利益。他们的互动以这个群体及治理协议为基础，对政策制定者而言是个自然的监管入口。〔44〕本文认为，当前影响主流区块链及元宇宙金融的“权力架构”主要由四个关键私主体构成，即核心技术开发团队、大型“矿工”、主流加密资产交易所、投资机构。这是元宇宙金融“再中心化”的重要主体。

元宇宙金融中，技术掌控权力，权力决定规则，规则塑造行为，行为产生结果。核心技术开发团队（通常以非营利基金会形式注册于瑞士等国）塑造元宇宙底层架构、业务本质和激励模

〔41〕 参见戴昕：《重新发现社会规范：中国网络法的经济社会学视角》，载《学术月刊》2019 年第 2 期。

〔42〕 参见前引〔30〕，普里马韦拉·德·菲利皮、亚伦·赖特书，第 192 页。

〔43〕 参见马治国、刘慧：《中国区块链法律治理规则体系化研究》，载《西安交通大学学报（社会科学版）》2020 第 3 期。

〔44〕 参见前引〔18〕，Sirio Aramonte、Wenqian Huang、Andreas Schrimpf 文，第 33 页。另一研究者亦指出实践中存在破坏区块链系统去中心化设计初衷的因素。参见前引〔36〕，威廉·马格努森书，第 298－301 页。上述研究指出去中心化金融存在“中心化主体”，但未系统思考如何规制之。

型。核心技术开发团队拥有元宇宙及区块链系统的“立法权”，奠定其“法律世界”——基于代码的规则体系，形塑交易行为。这些规则确立区块链系统行为模式和交易结构，是区块链系统的“宪法”，独立于现实世界的法律，依托日益增长的全球分布式算力而愈发稳定。元宇宙受益于区块链开发者推陈出新的技术迭代，最后构造独立于现实世界和开发团队自身的“平行宇宙”，即由代码规范的“元宇宙世界”。

与之相关，“矿工”是运维区块链系统的主体，遍布全球。拥有算力优势的大型“矿工”负责把特定时间段系统发生的交易信息记载到区块。为激励“矿工”竞争参与“挖矿”，提升区块链系统安全性，核心技术开发团队设定加密资产（数字通证）激励机制，让“矿工”利益得到保证，并吸引足够多“矿工”参与，技术开发团队预设挖矿难度动态调整，设定诸如比特币每四年发行量减半的规则，参与越早，获利可能越大。“矿机”算力越强，“挖矿”难度越大，区块链系统稳定性越高。〔45〕研究者指出，诸如以太币等加密货币和建于其上的去中心化金融协议依赖验证者或矿工作为中介机构，以验证每笔交易、更新区块信息。这些中介机构可选择添加到账本的交易及交易顺序，因此他们可以采用一些在传统市场可能属于违法的行为，比如抢先交易（front-running），这种获利结果被称为“矿工榨取价值”。就这种市场操纵行为需要针对这类中介机构采取新的监管方式。〔46〕

加密资产交易所决定哪个区块链系统发行的加密资产可在其平台交易。头部中心化交易所（如 Coinbase）及主流 NFT 交易平台（如 OpenSea）巨大的交易体量和交易深度为特定加密资产带来了价格发现、流动性、变现能力、投资价值和财富效应，从而吸引更多投资者投资区块链和元宇宙项目，持有或使用特定加密资产。财富效应直接影响区块链及元宇宙系统技术开发团队的后续积极性和用户人数，影响其成长和生命力。典型事例是原以太坊因“DAO 事件”硬分叉后，大部分矿工切换到新链时，部分矿工维持着旧链，他们在旧链挖出的币（ETC）在交易所无法交易，几乎没有任何价值，矿工无经济来源。在旧链即将消失时，当年全球最大的以太币交易平台 Poloniex（业界称“P 网”）宣布开始交易 ETC，ETC 因此具有流通价值，矿工们的生计得以为继，旧链算力迅速增强。〔47〕

公共区块链需要某种资源驱动，如以太坊需要类似于燃料性质的以太币驱动智能合约执行或每一步链上交易行为。一些加密资产长期成为投资或炒作对象，成为一些高风险投资者储藏价值或法币替代性支付的途径。人们获取此类加密资产的主要途径，一是“挖矿”激励所得，二是在各类交易场所购入。因此，主流加密资产交易所与大型“矿工”作为特定机构，可成为法律规制的有效“抓手”。元宇宙金融表面上高度去中心化，但大型“矿工”与主流加密资产交易所导致

〔45〕 以太坊 2.0 阶段将采用“权益证明机制”（POS），这一阶段质押巨额以太币作为验证节点的个体或机构拥有话语权，成为“再中心化”主体之一。研究者认为这类大型“矿工”为了金融利益，拥有足够权力，可能改变记载上链的信息。参见前引〔18〕，Sirio Aramonte、Wenqian Huang、Andreas Schrimpf 文，第 28 页。

〔46〕 See Raphael Auer，Jon Frost & Jose Maria Vidal Pastor，Miners as Intermediaries：Extractable Value and Market Manipulation in Crypto and DeFi，BIS Bulletin，16 June 2022. 研究者称，“挖矿业”集中对公共区块链去中心化的前提提出质疑，在以太坊权益证明（POS）机制下，以太币巨额拥有者促进不同程度的集中。此外以太坊基金会在以太坊生态系统中具有较强地位。参见〔美〕凯文·韦巴赫：《区块链与信任新架构》，杨东等译，机械工业出版社 2020 年版，第 95－96 页。

〔47〕 参见前引〔35〕，井底望天、武源文等主编书，第 80－81 页。

其“再中心化”。监管机构对交易所和“矿工”备案、登记、核准或管制，要求其提供大额加密资产流向信息登记，交易对手采取实名制，防止拥有算力优势的“矿工”发动“双花”攻击。对加密资产交易所的规制可参照金融监管法律体系，形塑交易所规则。如要求交易所比对与识别交易者身份，充提币身份验证、限时限额提币、提币黑地址（可能被黑客使用过的公钥地址）识别并拒绝服务等。

投资机构资金参与量直接影响区块链系统及元宇宙项目的研发、使用热度、知名度、系统迭代进度，加密资产（如元宇宙售卖的虚拟地块）价格上涨吸引“矿工”投入更多资金购买专用计算机设备“挖矿”，或投资人竞相购买加密资产，使区块链和元宇宙金融运行愈加安全稳健。多数知名区块链项目背后都有行业投资机构作为推手。通常，核心代码开发者决定元宇宙底层结构、激励机制与商业模式，但商业利益方面的诉求使得投资机构的意图必然形塑代码开发者的理念，影响元宇宙商业模式和应用。

通过规制行业头部投资机构（中心化实体），监管者有可能将元宇宙金融置于法律规制之下，借由中心化机构实施对元宇宙金融的规制。比如，自 2021 年以来，美国世可（Circle）公司发行受美国监管的中心化稳定币 USDC，其作为 DAI（去中心化稳定币）的质押比例不断上升。世可公司跟美联储充分合作，它的美元资产在美联储监管下，资产形态是美元和美国国债。在 USDC 份额占 DAI 的质押品一半以上时，DAI 事实上已被中心化的公司潜在支配。USDC 作为连接传统金融（中心化金融）与去中心化金融的媒介，提升传统金融机构对稳定币的采用率，帮助传统资金以合规方式获得元宇宙金融服务。在这一进程中，去中心化的稳定币主要由中心化机构的资产支持时，美国金融监管法律体系实际上经由受监管的稳定币向元宇宙金融渗透。与此类似，加密资产交易另一主流稳定币 USDT 由中心化的法律实体 Tether 公司经营。当元宇宙金融高度依赖这些稳定币时，也将受中心化金融与传统金融支配。

此外，还有一些边缘性私主体拥有小部分“权力”，并发挥着一定的影响力，比如主流区块链资讯媒体、区块链数据与安全分析公司及知名区块链浏览器等。综上，有效规制元宇宙金融，政府及法律应将核心技术开发团队、大型“矿工”、主流加密资产交易所和投资机构作为重点被规制对象，助推现实世界的权力以规训元宇宙系统。

（三）重点规制阶段的配置

加密资产与法币兑换是加密资产流通中至关重要的环节，也是加密资产及元宇宙各类数字创造（如在元宇宙的虚拟地块建造别致的虚拟建筑物并以 NFT 形式确权）完成价格发现的渠道。作为这一渠道的关键载体，加密资产交易所以及 NFT 交易平台已成为元宇宙金融的基础设施。这些载体承担加密资产变现和融资的功能，为元宇宙带来资金和创新动力，是投资人的变现途径。因此，政府规制元宇宙金融的重点阶段可置于元宇宙金融与现实世界的链接点——交易者以加密资产兑换法定货币（或现实世界的产品与服务）这一过程。监管机构难以监管元宇宙金融本身，但可对法币（现实世界）与元宇宙（虚拟空间）交互过程施加有效监管。监管机构通过授权合规、严格管控的中心化交易所或平台，创新探索实施特定加密资产“上市”和“退市”制度试点，间接将元宇宙金融纳入规制范围。在监管机构指导下制定交易所业务和技术标准通用规范、职业道德规范，强化各类审查制度，包括严格的用户身份识别机制、反洗钱机制、交易所网络安

全标准及交易资金合法性来源审查等，〔48〕处罚违法的交易平台。规制中心化交易所或平台，监管机构推动金融监管法律体系与元宇宙金融链接，使现实世界的法律向虚拟时空传递。对初始意图即为明确对抗审查与监管而生的加密资产（比如零币、门罗币等隐私币），〔49〕监管机构可直接要求交易所不得交易此类资产，限制元宇宙金融潜在风险（如洗钱）。

去中心化交易所无特定法律主体，允许用户保持匿名状态和抗审查，不必将现实世界真实身份与交易或账号联系，为元宇宙金融用户借机进行违法犯罪行为（洗钱等）提供便利。不过目前去中心化交易所影响力较为有限，交易量不可与中心化交易所同日而语，〔50〕但其运行特点挑战监管者能力，将成为监管者下一步规制的对象。在去中心化交易所发展壮大前，大力鼓励受监管的中心化交易所吸引大部分投资者，使现实社会的法律与元宇宙金融链接，不失为规制路径的首选。

综上，为提高效率，各类去中心化应用在治理机制方面不可避免地有“再中心化”特色，并非绝对“不可规制”。近年多数去中心化应用表层采取“去中心化”治理模式，项目迭代、参数变动及项目“财库”的代币调用等倚靠社区投票表决。持有去中心化项目发行的治理代币数量决定了投票权权重，然而，大量治理代币主要集中在核心代码开发团队、早期投资机构或应用项目重要参与者手中。〔51〕寡头式治理比大众共治具有更高效率，尤其是应对金融风险及时作出决策是去中心化项目存活的关键。这些因素决定了中心化治理色彩将是常态。因此，元宇宙的“去中心化”金融实质上多以“中心化”方式治理，这个悖论为元宇宙金融被有效规制提供了良途。

四、规制原则、方式和局限

（一）规制的基本原则

元宇宙金融尚在发展形成中，应对创新者与监管者间可能产生的对立情绪和立场予以警醒，其间应设定合理创新与监管博弈的空间。正常创新与监管博弈有益于理性地发展元宇宙金融。如专家所述，在比特币行业快速发展的地区，监管机构不可避免地面临两难选择。他们过早行动，在没有正当理由的情况下会使新技术受到旧规则的约束，就有可能扼杀创新或将其推行至其他司法辖区。但若监管者观望时间过长，公众将受到损害，到时候对现实存在且影响重大的行业提出监管要求的成本将会更高。〔52〕此外，有学者亦称，区块链开发活动激发在全球范围内分布与管

〔48〕 对此可参考日本与美国纽约州的监管经验。参见邓建鹏、孙朋磊：《区块链国际监管与合规应对》，机械工业出版社2019年版，第63－70页、第89－94页。

〔49〕 研究者指出门罗币隐藏所有交易信息，为洗钱犯罪活动提供便利。参见前引〔36〕，威廉·马格努森书，第243页。

〔50〕 研究者统计去中心化交易所交易量占加密资产总交易量的10％以内。参见前引〔18〕，Sirio Aramonte、Wenqian Huang、Andreas Schrimpf文，第26页。

〔51〕 比如在2019年10月举行的决定去中心化银行MakerDAO发行的稳定币DAI利率是从12％提升到13.5％还是降到5.5％的投票中，本来只有两千四百多张投票，随后一个持有人提交四万多张投票，占总投票数的97％。参见前引〔15〕，郑磊文。Uniswap在2021年6月就旨在为监管政策制定者普及、推动DeFi而筹款的基金，以投票方式通过由Uniswap财库拨款100万枚UNI以运作该基金的提案。该提案投票过于集中，有明显中心化倾向。参见https://www.8btc.com/article/6660705，最后访问时间：2021年7月14日。

〔52〕 参见前引〔46〕，凯文·韦巴赫书，第138页。

辖权竞争。美国在早期互联网行业的主导地位为美国带来了重大利益，包括经济利益和全球软实力。〔53〕区块链技术、虚拟货币在金融科技领域深受关注。各国展开的制度竞争越发突显。2022 年 3 月，美国公布《数字资产行政命令》，其强调将在数字资产创新和治理中继续发挥领导作用，首先将保护美国消费者、投资者和企业的政策目标放在首位，然后强调维护美国和全球金融稳定，降低非法金融和国家安全风险，负责任地引领创新，强化美国在全球金融体系、技术和经济竞争力方面的领导地位。〔54〕2022 年 4 月，英国财政部经济部长约翰·格兰（John Glen）在金融科技周的创新金融全球峰会上发表演讲，表示会对加密资产市场给予充分的政策和法律支持。〔55〕

这表明世界经济体大国希望通过有效监管实践，在虚拟货币全球治理中发挥领导作用。晚清对外贸易史及公司制度史的经典研究充分表明，国与国间竞争的核心是制度间竞争。〔56〕在当前国际竞争背景下，发挥政策与制度优势，提升我国在元宇宙金融乃至金融科技领域国际竞争力，具有紧迫性和必要性。规制的内涵不只是约束和禁止，也包括激励与促进。政府不应仅考虑为抑制风险而行使监管的权力，还应考虑如何利用适当的法律与政策促进元宇宙玩家的创造力，推动虚拟空间数字财富增长。近十年来，金融科技等领域的中国监管政策存在“一抓就死，一放就乱”治乱循环，易增加社会成本，打破市场主体预期。作为金融科技与数字经济时代的创新代表之一，中国对元宇宙金融应设定包容的规制原则，对元宇宙金融创新及难免招致的风险予以适度包容，在控制风险底线、保障用户合法权益的前提下，鼓励元宇宙金融创新。

（二）规制的几种途径

网络法专家论述了规制互联网的四种方式，即国家法律、市场、社群规范和架构。〔57〕这为元宇宙金融规制方式提供部分启示。区块链技术及元宇宙金融应用仍处高速发展中，远未定型。研究者谓，面向公众的区块链网络必须满足哪些内部治理要求，现有法律并无规定，因此使用者只能任凭网络创始人和开发者随意制定内部治理框架并选择通过技术代码实施。〔58〕一些区块链项目创始人和开发者的任性和随意性令人触目惊心。比如，Sushiswap 匿名创始人糯米（Chef Nomi）于 2020 年 9 月 5 日从 Sushiswap 的流动资金池中提取 Sushi（Sushiswap 项目的数字通证）套现成价值约 1300 万美元的以太币，导致 Sushi 市场价格 18 小时内暴跌 73%以上。第二天糯米突然宣布将自己的项目控制权（即私钥）交给加密资产交易所 FTX 的 CEO 萨姆（Sam Bankman-Fried）。〔59〕

〔53〕 参见前引〔46〕，凯文·韦巴赫书，第 151 页。

〔54〕 See The White House, Executive Order on Ensuring Responsible Development of Digital Assets, 2022-03-09, available at https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/, last visited on May 29, 2021.

〔55〕 See John Glen, Keynote Speech by John Glen, Economic Secretary to the Treasury, at the Innovate Finance Global Summit during Fintech Week 2022, 2022-04-04, available at https://www.gov.uk/government/speeches/keynote-speech-by-john-glen-economic-secretary-to-the-treasury-at-the-innovate-finance-global-summit, last visited on May 29, 2021.

〔56〕 参见方流芳：《公司词义考：解读语词的制度信息——“公司”一词在中英早期交往中的用法和所指》，载《中外法学》2000 年第 3 期。

〔57〕 参见前引〔37〕，劳伦斯·莱斯格书，第 360-366 页。

〔58〕 参见〔英〕凯伦·杨：《区块链监管：“法律”与“自律”之争》，林少伟译，载《东方法学》2019 年第 3 期。

〔59〕 See Fishy Business: What Happened to $1.2B DeFi Protocol SushiSwap Over the Weekend, available at https://www.coindesk.com/sushiswap-liquidation-weekend, last visited on Jun. 5, 2021.

有学者认为，在创新初生期，行政机关承担主导性规制，大多以指导性规制方式展开；在创新成熟期，创新本身的规制问题点充分发酵，可能需要将部分规制内容上升为立法；司法机关则在创新各个阶段承担裁判性规制，作为以上两种规制方式的辅助。随着信息革命到来，复杂变动的社会事实令指导性规制在整个规制框架内扮演着重要角色。〔60〕首先，元宇宙金融处于创新初生期，针对行业风险与问题，监管机构通常处于规制的主导地位，在具体方法上，以非正式指导或正式法令、指引影响区块链代码规则、技术安全标准与社区自治规范，前者如发布技术白皮书，会议讨论和风险提示等方式，后者如与技术、代码安全等相关的国家标准。这些方式有助于引导元宇宙社区自治规范以程序正义的方式制定规则和决策，把上述规则和决策转换成代码，然后将这些代码部署到区块链系统和智能合约中，同时监管者应鼓励行业进行事前专业的智能合约安全审计，排查各类漏洞。

政府部门引导企业制定区块链与元宇宙的技术标准，通过规制技术，间接规制元宇宙的业务与行为。如在 2020 年 7 月，中国人民银行印发《关于发布金融行业标准推动区块链技术规范应用通知》和《区块链技术金融应用评估规则》（JR/T 0193—2020）。该标准规定了区块链技术在金融领域应用的实现要求、评估方法、判定准则等，适用于金融机构开展区块链技术金融应用的产品设计、软件开发和系统评估。该标准从基本要求、性能、安全性等方面为去中心化金融应用提供客观、公正、可实施的评估规则，保障去中心化金融设施与应用的安全稳定运行，促进去中心化金融应用健康有序发展。〔61〕不过，中国已有规则主要针对持牌金融机构开发联盟链而设定，表达监管者规制区块链的初步尝试，对公有链影响力较有限。

其次，通过修订法律、提升监管技术，推动元宇宙金融与监管科技结合，推动主权国家逐渐将元宇宙置于法律规制之下。元宇宙金融稳健发展，需为加密资产和智能合约构建合适的法制框架，包括加密资产及稳定币的法律属性，智能合约的法律地位及其法律救济等。在监管技术方面，多数区块链上的信息透明可查询、可追踪。监管机构在一些区块链安全与数据分析技术公司的协助下，解析诸如比特币或以太坊等的账本数据，追溯定位特定公钥地址与使用者的对应关系，最后揭示当事人的真实身份，打击从事洗钱、传销、违禁品交易及通过病毒软件勒索比特币等行为的罪犯。〔62〕监管机构在区块链安全技术公司帮助下，给一些攻击者（黑客）的相关公钥地址打上标签，一旦这些被“标签”的地址开始转账，系统会自动标记相关交易地址，追踪和监控资金流向，监控目标地址交易，追踪主体信息，锁定犯罪分子。尤其是当用户由虚拟空间进入现实世界时，如将加密资产兑换为法币，或用加密资产购买现实世界的商品与服务，其真实身份将显露出来。加密资产在区块链系统中的发送与接收，与传统的网络 IP 地址类似。理论上而言，监管机构可以跟踪这些 IP 地址，将加密资产流向置于规制范围之中。

最后，信息科技巨头基于其强大的技术研发力量，为元宇宙构建提供各种硬件和软件，必然

〔60〕 参见王首杰：《创新规制的时间逻辑》，载《华东政法大学学报》2022 年第 3 期。

〔61〕 参见《〈区块链技术金融应用 评估规则〉金融行业标准正式发布》，载 https://www.cfstc.org/jinbiaowei/2929436/2976686/index.html，最后访问时间：2020 年 8 月 27 日。

〔62〕 美国执法机构曾在 2021 年通过技术手段，将黑客以勒索病毒获取的比特币赎金成功“夺取”回来。See Eric Tucker, US Recovers Most of Ransom Paid after Colonial Pipeline Hack, available at https://apnews.com/article/technology-business-government-and-politics-8e7f5b297012333480d5e9153f40bd52, last visited on Jun. 8, 2021.

影响元宇宙金融规则制定，这为现实世界的法律与监管政策规制元宇宙金融提供了路径。相关部门可鼓励商业机构进军元宇宙，探索商业应用，在技术标准与代码规则等领域发挥影响力；推动中心化商业机构（封闭式元宇宙）与开放式元宇宙融合，影响元宇宙“再中心化主体”，以现实世界的法规塑造开放式元宇宙规则框架；监管机构推动封闭式元宇宙在整个元宇宙规则制定中的话语权，使元宇宙金融与现实世界法规协调。比如，鼓励元宇宙去中心化金融与传统金融融合，使传统金融合规业务向元宇宙渗透。有研究者称，去中心化金融可利用传统金融的资产以合规方式实现扩张，打造虚实结合的数字金融环境。在一些国家，去中心化金融服务已打通虚拟与现实世界。一些加密货币模仿现实金融体系要求，建立资产储备制度，将加密货币等对应一定比例的现实资产与商品。〔63〕

（三）规制局限性的思索

头部加密资产交易所是规制的重要抓手，但也存在局限性。反洗钱金融行动特别工作组（FATF）建议监管机构记录加密资产用户的资料，使他们能更好地识别犯罪活动。其在 2020 年 9 月中旬的一份报告中指出，将用户交易活动与其个人资料对比，可发现某些危险行为和特征，包括用户是否有犯罪记录，或是否活跃在与非法活动相关的网站和论坛上。监管机构也需要关注用户使用比特币或以太坊购买诸如门罗币或零币等行为，后两者会混淆第三方的交易活动。〔64〕将主流加密资产交易所、加密资产钱包提供者纳入监管范围，有助于减少上述风险。FATF 在 2020 年下半年还计划为各国政府制定关于共享虚拟资产服务提供者信息的全球框架，此类提供者包括加密资产交易平台、钱包服务提供者及稳定币发行方。〔65〕当然，多数加密资产交易所面向全球客户提供金融服务，鉴于各国监管标准差异甚大，单一国家如何有效规制境外交易所成为时代挑战。由于交易所的全球分布式办公，办公机构与金融业务跨越多个司法管辖区，容易规避特定国家的监管。更进一步，某些境外交易所可能直接注销中国境内的关联公司，从而对中国司法机关的管辖或案件执行造成困难。

有学者提出政府可监管开发区块链协议和智能合约的人。〔66〕例如，在各国监管者呼吁或压力之下，以太坊核心技术开发人员可能通过提出部分代码修订，使以太坊部分代码融合现代法律规则，但这能否完全收效，尚有待观察。元宇宙与区块链的规范是通过代码规制社群，发挥着独立于现实社会法律体系的作用。以太坊等主流区块链背后有影响力巨大的核心技术开发团队，其通常依托于非营利基金会，获取基金会资助。核心技术开发团队在元宇宙及区块链发展方面拥有很大话语权和影响力，因此，技术团队负责人可成为法律规制的对象。

不过，这种规制意图可能部分落空。其一，代码规则和智能合约内容涉及大量机器语言，内容极为复杂，难以事先审查。政府全面监管一国范围内所有代码开发人员，一是增加巨额监管成本，二是直接阻碍区块链与元宇宙技术创新。其二，一些代码开发者一开始便有意隐匿真实身份

〔63〕 参见前引〔15〕，郑磊文。

〔64〕 See User Profiling Can Help Regulators Identify Illegal Crypto Activity, Says FATF, available at https://www.coindesk.com/user-profiling-regulators-cryptocurrency-crime-fatf, last visited on Nov. 26, 2020.

〔65〕 See FATF Plans to Strengthen Global Supervisory Framework for Crypto Exchanges, available at https://www.coindesk.com/fatf-plans-to-strengthen-global-supervisory-framework-for-crypto-exchanges, last visited on Nov. 26, 2020.

〔66〕 参见前引〔30〕，普里马韦拉·德·菲利皮、亚伦·赖特书，第 199 页。

（如“中本聪”），致监管失效。其三，大多数具有世界影响力的区块链和元宇宙项目创新应用的核心代码开发者分布在欧美等发达国家。无论是主流共识算法，还是跨链、侧链等拓展技术或元宇宙金融重要生态，基本由国外技术团队主导。对中国监管机构而言，规制境外核心技术开发人员可能力不从心。其四，多数核心技术开发团队组织并非固定法律实体，而是松散组织，开发者随时可自由加入或退出团队。这种自治组织形式的运作遍布不同司法管辖区，没有董事会或经营者这样的公司管理层，而是通过民主参与、代码规则、算法与分布式共识管理，使用智能合约收集成员投票。组织成员使用代码和智能合约管理事务，智能合约设定的条款至高无上，代码规则而非法律文件被用以界定成员间权利和义务。这种自治组织作为协调全球投资和社区治理的模式，可用于包括管理区块链项目运营和资本运作等许多目的，这种运营特色对中心化的规制方式造成障碍。

如特定区块链系统大部分核心技术开发团队或系统全球算力的51%以上集中在某一国家，该国政府可以通过规制技术开发团队或“矿工”的方式，有可能部分规制元宇宙金融。比如，迫于监管者压力，技术开发团队和“矿工”同意修订某些区块链底层协议，但也可能带来巨大代价。一是此种行为成本高昂，诸如对比特币新区块的修订，要汇集比特币系统算力的51%以上，其成本或将近百亿美元；二是这将大幅度降低区块链和元宇宙极高的技术信用，直观表现就是相关币价可能暴跌，元宇宙加密资产甚至有归零风险，严重侵害全球合法持有者的权益，可能招致全球投资者国际诉讼风险，这将使监管机构对此种规制投鼠忌器。

元宇宙金融经历着“去中心化—再中心化—再去中心化”的演化，加剧“不可规制性”，导致金融监管法律体系与代码规则间的紧张关系。以MakerDAO为例，治理在其生态系统中有着重要角色，但代币持有者投票治理过程漫长，为此，几个核心小组的参与确保治理得到运行，再加上其质押资产近一半为中心化的美元稳定币USDC，这为现实社会法律规制创造了机会。不过，这一中心化治理风险为更加去中心化的治理模式，即借贷协议Liquity提供了机遇。Liquity系统选择无人治理的模式，Liquity协议参数要么一成不变，要么完全由算法控制，质押资产则是极具去中心化特色的以太币。Liquity系统的借贷费和赎回费由数学算法决定，让交易者信任代码按承诺执行，算法、代码和数学的信用取代了人的信用，因此，特定主体的人为因素在系统运行中被降到极致。

作为早期成功的风险投资机构，Andreessen Horowitz（业界简称“A16z”）持有Compound、Uniswap等去中心化金融项目的大量代币。A16z建立授权计划，将这些代币半数以上的投票权委托给非营利组织、德国电信等全球企业、加密初创公司及崭露头角的社区领袖，被委托人可以合适方式独立于代币持有者投票。〔67〕授权计划改变了A16z在Compound、Uniswap等项目中投票权过度集中的状态，在保证投资机构盈利的前提下，淡化自身在上述项目治理机制的中心化角色，这是典型的刻意“再去中心化”。有学者认为，当去中心化自治组织无中心权威，实现分布式决策后，去中心化自治组织有限合伙定性的组织基础或成员结构已然丧失，而我国现有法人形态是中心化科层式的制度设计，与其去中心、去信任等本质特点不符，无法直接套用。〔68〕元宇

〔67〕 参见《A16z DeFi委托“开源”计划详解》，载https://www.jinse.com/blockchain/1149655.html，最后访问时间：2021年9月5日。

〔68〕 参见郭少飞：《再论区块链去中心化自治组织的法律性质——兼论作为法人的制度设计》，载《苏州大学学报（哲学社会科学版）》2021年第3期。

· 51 ·

宙金融“再去中心化”，本质是“可规制性”向“不可规制性”转型。

近年一些诉讼表明，一些区块链系统私权力主体试图规避或抵制在现实社会承担法律责任的要求。比如，美国证券交易委员会（SEC）认为瑞波（Ripple Labs）公司未证券注册，擅自发行加密资产，向当地法院提起诉讼，〔69〕要求瑞波公司承担证券法上的相关责任。针对 SEC 的起诉，瑞波公司认为瑞波币价格波动主要由二级交易市场决定，投资者并非依赖瑞波公司（中心化主体）的努力获益，因此瑞波币不符合“豪威测试”第四项要求。〔70〕瑞波公司声称在瑞波币价格影响方面居于边缘角色，这与事实并不符。区块链项目开发者精心构建代币系统，力图向法院证明其发行的代币不符合“豪威测试”标准，以规避证券法约束。〔71〕

权力即责任，权力越大，责任越大。元宇宙中心化主体“再去中心化”，试图规避现实社会责任，形式上避免成为中心化权力来源。知名区块链系统创始人及近年一些知名去中心化金融应用创始人保持匿名，加剧了区块链和元宇宙的“不可规制”。综上，元宇宙金融将大部分被规制，但难以完全驯服。

五、结　论

区块链为元宇宙提供去中心化金融业务的技术基础，元宇宙金融逐渐成长为与传统金融平行的新体系，各种应用组合形成高度创新的生态，客观上出现元宇宙与政府争夺虚实空间的控制权和治理权的状况，固有金融监管法律体系难以完全适用。现实社会法律与监管规则尝试规制这种新业态时，需从金融包容角度进行思考。如有学者认为，对区块链金融衍生品法律评价应多元，不能因其可能诱发犯罪就拒绝赋予其合法地位，对其评价要考虑未来技术发展需要，要考虑对我国实体经济是否能产生促进作用，要考虑相关行为是否具有严重的社会危害性等诸多因素。虽然政府曾多次出台相关文件规范加密资产，禁止金融机构开展与比特币相关的业务，但是政府的这种政策性叫停并未从本质上解决问题，只有良好的法律才能为其发展提供强有力的保障。〔72〕我国当下在虚拟货币领域采取的“禁令型”监管是暂时的政策选择与监管观望，后续有必要持续探索更加符合金融科技风险特征的治理机制。〔73〕元宇宙金融犹如空气般弥散于世界，打破市场、企业、社会和国家的界线，自生代码体系和法律制度相对独立，但其并非不可规制，原因是元宇宙金融“再中心化”，即核心代码开发者、头部加密资产交易所、大型“矿工”和主流投资机构等私权力主体掌控元宇宙。

元宇宙金融突破传统金融业态，使金融监管法律体系不得不回应和重构。元宇宙金融底层技术

〔69〕 See SEC, Complaint: Ripple Labs, Inc. (“Ripple”), Bradley Garlinghouse and Christian A. Larsen, available at https://www.sec.gov/litigation/complaints/2020/comp-pr2020-338.pdf, last visited on Jan. 5, 2021.

〔70〕 See Ripple, Our Statement on Recent Market Participant Activity, available at https://ripple.com/ripple-press/our-statement-on-recent-market-participant-activity/, last visited on Jan. 5, 2021.

〔71〕 See Neil Tiwari, The Commodification of Cryptocurrency, 117 *Michigan Law Review*, 615-617 (2018).

〔72〕 参见杨玉晓：《区块链金融衍生品刑法规制研究》，载《重庆大学学报（社会科学版）》2020 年第 6 期。

〔73〕 参见邓建鹏、马文洁：《虚拟货币整治的法治思考与优化进路——兼论对金融科技的“禁令型”监管》，载《陕西师范大学学报（哲学社会科学版）》2022 年第 3 期。

架构决定特定国家法律规制存在困难，需要监管者重点厘清可规制对象，提升监管科技水平和规制能力，依托国际间政府组织，推动金融监管国际协作，同时应充分理解当前规制方式的限度。元宇宙金融可能将传统金融业务边界拓展至无限，出现元宇宙世界与现实世界双重构造，二者行为模式与治理规则交互形塑人们的社会关系。固有金融监管法律体系并非应对元宇宙而生，很难应对其风险，因此有必要全面思考这一领域的技术特点和商业模式。有学者认为，信息革命的加速到来，中国法学的自主不足和数字时代的重大挑战，为当下法学研究带来了双重压力，同时也带来了独特机遇，适时转换研究理念就成为一种必然抉择。〔74〕元宇宙金融正在生成新型财产权利关系，奠定前所未有的权利义务结构、复杂法律属性和金融业态，与现实社会有不一致的构造、规则生成与行为模式，经历“再中心化”与“再去中心化”的动态演化。“一刀切”式的固有整治思维并不管用，法学家需要极为精细的研究，紧密跟踪和研判元宇宙金融发展趋势，加强对区块链技术的知识储备，深化法学（及金融监管）意义的研究视角，从而贡献更为有效的规制理论体系。

Abstract：The core of metaverse finance is decentralized finance based on blockchain technology. This new type of finance has created a low-cost and high-efficiency operation method, and it has characteristics such as no access threshold, unclear identity of the global participants, tamper-proof, anti-censorship, self-creation of rules and automatically running, etc., which have impacted the financial supervision legal system. However, metaverse finance is not absolutely unregulated. It is undergoing an evolution process from “decentralization” to “recentralization”. Regulators should take the “recentralized” organizations of metaverse finance into regulation, through informal guidance, promulgate national standards and formal legislation on blockchain technology and code security, promote the integration of traditional finance and metaverse finance, to which affect code rules, improve technical security and shape community autonomy norms. At the same time, the technical characteristics of the blockchain and the “re-decentralization” evolution of metaverse finance determine that it cannot be completely regulated by law in a long time.

Key Words：metaverse finance, blockchain, recentralization

（责任编辑：李　敏　赵建蕊）

〔74〕 参见马长山：《迈向数字社会的法律》，法律出版社 2021 年版，第 19 页。

财经法学 No. 5，2022
pp. 54 - 69

元宇宙对著作权法的挑战与回应

张金平 *

内容提要：元宇宙是跨多个司法管辖区的去中心化虚拟现实世界，供来自全球的用户利用元宇宙平台提供的工具自由创建和交易虚拟现实物品，因而可为人们提供与现实世界无异的创作环境。然而，元宇宙跨境去中心化运营会对著作权法的地域性带来一系列的挑战，导致元宇宙中作品著作权的归属、著作权具体权利内容和保护程度、著作权的利用以及侵权救济都会出现不确定性，但通过科学解释著作权基本原理和国际私法规则，并结合技术解决方案仍可以妥善应对。

关键词：元宇宙　著作权　NFT

一、元宇宙提出的著作权问题

元宇宙（metaverse）并非2021年才凭空提出。早在1992年，尼尔·斯蒂芬森在小说《雪崩》中就首次提出这个概念。在该小说中，尼尔将元宇宙描绘成一个由计算机协会全球多媒体协议组织管理的虚拟空间，当用户进入元宇宙时看到的是一条大街，楼宇和电子标志牌延伸到黑暗之中，消失在星球弯曲的地平线之外，用户实际看到的是一幕幕电脑图形表象，即一个个出自各大公司设计的软件用户界面。若想把这些东西放置在元宇宙大街上，各家大公司必须征得全球多媒体协议组织的批准，还要购买临街的门面土地，得到分区规划许可、获得相关执照；有关土地购买的资金全部流入由该组织拥有和运营的一项信托基金，用于开发和扩充机器设备，维持大街继续存在。在元宇宙中，每个用户都是编程高手，所以这片乐园显得品味不凡。〔1〕

* 张金平，中央财经大学法学院副教授。

本文为中央财经大学青年教师发展基金资助项目“人工智能时代著作权制度的挑战与应对”（QJJ2003）、国家社科基金重大研究专项“社会主义核心价值观视角下个人信息保护立法研究”（20VHJ008）的阶段性成果。

〔1〕 参见〔美〕尼尔·斯蒂芬森：《雪崩》，郭泽译，四川科学技术出版社2009年版，第29－32页。

虽然元宇宙目前尚未完全构建出来，但已经有三次重大尝试。第一次突破性的尝试是林登实验室2003年创建的虚拟现实空间《第二人生》。〔2〕林登实验室突破了传统游戏开发商对游戏内容和故事完全掌控的做法，仅为用户提供可购买的虚拟土地、可自由创建三维内容的工具，以及可自由交易创建内容的平台和可兑换现实货币的林登币，从而让用户充分根据自己的意愿去创建内容并与他人交互。根据林登实验室2022年的数据，《第二人生》全球拥有5000万用户，用户自创20亿个虚拟物品，这些虚拟物品年交易额达到6.5亿美元。〔3〕不过，这个元宇宙雏形仍然是中心化的大型在线虚拟现实空间，用户仍然要遵守林登实验室制定的平台规则，而且用户创建的内容无法在其他平台共享使用。第二次尝试是2017年开发的Decentraland。不同于基于中心化管理的《第二人生》，Decentraland基于区块链以太坊而创建，采用“去中心化自主组织”（decentralized autonomous organization，DAO）来管理，用户可以利用NFT技术交易自主创建的虚拟物品，〔4〕还可以成为Decentraland的成员来参与管理。〔5〕Decentraland使用以太坊钱包作为用户在元宇宙中的账号，为与其他同样使用以太坊创建元宇宙的平台进行跨平台交互提供了可能。第三次尝试则是扎克伯格2021年10月对元宇宙虚拟现实的设想。他通过长达77分钟的视频阐述了更为贴近尼尔·斯蒂芬森在《雪崩》中所要构建的元宇宙，即元宇宙有且只有一个，是由多平台共建、可互联互通的虚拟现实世界，而且用户在任一个元宇宙平台创建的内容都可以直接在另一个元宇宙平台使用。〔6〕

基于上述有关元宇宙的设定，我们可以结合作品创作、管理、利用和保护四大制度归纳元宇宙的特点。〔7〕一是提供用户自我创作的充分自由度，即用户利用元宇宙平台提供的物品编辑器可以编辑三维虚拟物品。只要满足独创性，这些物品可以构成作品。二是具备社交属性，用户通过作品在多个元宇宙平台之间无缝传播自己的思想表达，并在好友或者粉丝中建立声誉。〔8〕三是提供用户对其创设内容变现的环境和机会，即用户利用元宇宙平台提供的数字货币可以自主对虚拟物品标价并与其他用户交易，这些数字货币可以与现实货币兑换。〔9〕从作品交易的角度而言，用户可以通过作品著作权许可或转让的形式获得版税收入。四是可以实现去中心化管理。通过成为去中心化组织成员的形式，用户可以享有对元宇宙尤其是用户自建内容的运营和管理的决定权。从作品保护的角度而言，用户作为去中心化管理的成员更有可能形成有利于作品在元宇宙中的创作、管理、利用和保护的平台规则共识，例如将作品交易中介费降低到让这个交易系统可

〔2〕 See Cory Ondrejka, Escaping the Gilded Cage: User Created Content and Building the Metaverse, 49 *New York Law School Law Review* 81, 87 (2004).

〔3〕 See Linden Lab, Tilia Partners With Unity to Power Virtual Economies for Game and Metaverse Developers, available at https://www.lindenlab.com/releases/tilia-unity-partnership, last visited on Jul. 11, 2022.

〔4〕 See Decentraland, White Paper, 2017, pp. 5－14.

〔5〕 See Decentraland, DAO, available at http://dao.decentraland.org/en/, last visited on Jul. 11, 2022.

〔6〕 不过扎克伯格希望用户在元宇宙的化身也采用真实世界的身份和外形，而且也更倾向于通过新成立的Meta公司来主导元宇宙内容的构建。See Meta, The Metaverse and How We'll Build It Together, Connect 2021, available at http://www.facebook.com/facebookrealitylabs/videos/561535698440683/, last visited on Jul. 11, 2022.

〔7〕 这里借鉴了韩国李林福先生提出的元宇宙三大要素，即自由度、社交、收益化，但他并未从著作权法的角度加以解读。参见〔韩〕李林福：《极简元宇宙》，黄艳涛、孔军译，中译出版社2022年版，第36－39页。

〔8〕 创作者声誉需要在社交的环境下才能形成，如果作品仅对自己可见那么难以形成规模化创作的内驱力。

〔9〕 在国内目前尚不允许数字货币与现实货币兑换，但国家已经开发和采用数字货币，未来数字货币可作为交易货币。

以持续运转的程度即可。

不过，元宇宙的去中心化跨境运营与著作权法的地域性会产生一定冲突。这些冲突至少可以归纳为三大方面：〔10〕一是每个国家对作品的归属安排不尽相同，为了元宇宙全球同步运营，可能需要作品著作权统一归属的安排；二是作品的全球跨平台展示和传播涉及的具体著作权有所不同，例如各国采用不同的著作财产权来控制作品交互式传播，这对作品全球统一许可或转让带来一定的难度；三是元宇宙中散布全球的用户发生著作权侵权如何确定管辖和准据法，一旦确定侵权，元宇宙采用的交易记录不可篡改的区块链技术可能会对停止侵权等侵权责任的承担造成障碍。考虑到多平台互联互通并去中心化管理的元宇宙尚未完全建成，本文在对上述问题进行讨论时，将围绕中心化的《第二人生》和去中心化的 Decentraland 两个代表性元宇宙模型展开交叉分析，希望能够发掘元宇宙开发不同阶段上述著作权问题的不同解决方案，求教于各位方家。

二、作品著作权归属的挑战

基于著作权的绝对权属性，元宇宙中的作品创作完成即产生著作权，不因平台规则而消灭，但对这些作品在全球的统一著作权归属仍要基于《伯尔尼公约》相关规则来解决。〔11〕

（一）用户创作行为的决定性

《伯尔尼公约》规定只要作品创作完成，作者就对其作品享有著作权，不需要通过任何登记或审批等行政程序。〔12〕因此，在现实世界中，著作权始于作品创作这一事实行为。对于元宇宙，我们假定包括我国政府在内的各国政府都承认元宇宙的物品可以获得现实世界的价值，〔13〕那么用户创作的虚拟物品就不仅仅停留在虚拟空间，进而可通过赋予著作权的形式激励更多作品在元宇宙空间内的创作，打破过去由游戏开发商集中开发和控制的单一局面。

在元宇宙中，用户的哪些行为构成著作权法意义上的创作行为？在传统大型网络游戏构建的虚拟现实空间中，用户只能根据游戏开发商设计的内容和故事，进行竞技或者升级打怪，但这些行为都不是对游戏内容的创作。相比之下，元宇宙开发平台突破传统游戏开发商单方集中式创设内容的局限性，提供用户创制虚拟物品的工具或者编辑器，让用户创作更为丰富和复杂的虚拟现实世界。例如，林登实验室开发的《第二人生》直接提供游戏内的 3D 实时编辑器和脚本编辑工具，用户注册后就可以实时创制虚拟物品，并可以通过脚本程序设置指令让这些虚拟物品动起来。而且，林登实验室也不对用户创制内容设置单独的提交和审批程序。〔14〕相比之下，Decentraland 在提供创制物品的编辑器和脚本程序的同时，〔15〕还提供了建造虚拟物品的 3D 模型和材

〔10〕 元宇宙中可能涉及人工智能生成物的著作权问题，但这个问题脱离元宇宙也同样成立，所以不再单独分析。

〔11〕《与贸易有关的知识产权协定》（TRIPs）要求成员国遵守《伯尔尼公约》规定的义务，所以在作品归属、权利保护程度、准据法等方面的规则都取决于《伯尔尼公约》。

〔12〕 参见《伯尔尼公约》第 5 条。

〔13〕 该问题超出本文有关著作权的探讨范围。

〔14〕 参见前引〔2〕，Cory Ondrejka 文，第 87 - 93 页。

〔15〕 参见前引〔4〕，Decentraland 书，第 10 页。

料的在线内容库，并兼容外部 3D 模型和材料内容库，〔16〕让用户创建内容的门槛进一步降低，同时还可以借助 NFT 技术让创建内容变得可特定化。〔17〕因此，在元宇宙平台中，用户的创作行为可以是完全自我创作原始作品的事实行为，也可以是在他人创制的 3D 模块基础之上创作演绎作品的演绎行为。世界各国著作权法都普遍承认这两类产生作品著作权的创作行为，只是演绎作者在行使演绎作品著作权时必须尊重被演绎作品的著作权。

创作者对具备独创性的虚拟物品享有著作权。一般而言，用户在元宇宙中创作的虚拟物品主要包括化身的造型及其装饰品、虚拟土地上的建筑物和建筑物内部和周边可以展示的任何跟真实世界物品外观类似的物品，包括墙上的广告和其他 2D 画面、地面上静态或动态的 3D 物品。〔18〕其中，化身造型及装饰品是以线条、色彩或其他方式构成的有审美意义的立体造型艺术，可以作为美术作品得到保护。〔19〕虚拟建筑物因表现出审美意义而可构成建筑作品得到保护。〔20〕静态物品如以一定比例仿照现实物品的形状和结构则可以构成模型作品。〔21〕动态物品涉及脚本程序，可作为计算机软件得到保护。〔22〕在这些虚拟物品是否具备作品独创性的判断中，各国著作权法虽有差异，但随着《伯尔尼公约》和《与贸易有关的知识产权协定》（TRIPs）对各国著作权法的融合，这种差异基本可以忽略，只要能够体现出作者在创作素材的选择和安排中的个性化即可。〔23〕当然，仅仅复制他人 3D 模块不构成演绎，简单组合他人 3D 模块也因不具有独创性而无法产生著作权。

（二）平台规则不影响用户著作权的产生

著作权作为财产权具有绝对性，其权利的产生、权利的类型和保护期等不因私人的意志而变化，所以平台一旦提供用户创作作品的工具并允许这些作品可与现实世界交互，那么用户因创作而产生和享有的著作权就不因平台规则而消灭或者剥夺。在传统游戏中，游戏运营商为了绝对控制游戏，往往在平台规则中禁止玩家交易游戏装备，一旦玩家被发现通过第三方交易平台或者线下交易游戏装备就可以封号，剥夺用户参与游戏的权利，法院也普遍承认传统游戏运营商通过格式合同作出的这种限制。〔24〕相比之下，元宇宙开发平台如果赋予用户创制内容的工具，同时又在其平台规则中不承认用户对其创制内容享有著作权，那么该服务协议的相关条款可以根据格式条款的相关规则判定为无效，即因构成排除和限制用户主要权利而无效。〔25〕

有鉴于此，目前致力于打造元宇宙的《第二人生》和 Decentraland 的平台规则都承认用户对

〔16〕 例如 Sketchfab 的 3D 材料库。

〔17〕 NFT 技术在第三部分再展开介绍。

〔18〕 元宇宙中的音乐往往是从现实世界中创作的音乐嵌入，因而这些音乐脱离元宇宙可以单独保护。元宇宙中用户在其虚拟土地上创作的连续动态画面也可以构成视听作品获得保护。

〔19〕 参见《著作权法实施条例》第 4 条对美术作品的定义。

〔20〕 参见《著作权法实施条例》第 4 条对建筑作品的定义。

〔21〕 参见《著作权法实施条例》第 4 条对模型作品的定义。

〔22〕 参见《计算机软件保护条例》第 3 条。

〔23〕 不过，李明德教授认为作者权体系国家在提供著作权和相关权二分保护的框架下，作品的独创性要求显然要高于版权体系下作品的独创性。参见李明德：《体育赛事直播画面的作品属性认定》，载管育鹰主编：《知识产权审判逻辑与案例：著作权卷》，法律出版社 2022 年版，第 18－20 页。

〔24〕 参见“李宏晨与北京北极冰科技发展有限公司娱乐合同纠纷案”，北京市第二中级人民法院（2004）二中民终字第 02877 号民事判决书。

〔25〕 参见《民法典》第 497 条。

其创作内容的著作权。其中，《第二人生》最新的平台规则并未直接强调用户对其内容享有著作权或其他知识产权，而是仅仅规定“您通过您的账号或使用 Tilia（《第二人生》开发商林登实验室的下属子公司）服务而提交的细节、信息或者其他数据享有所有权”〔26〕。相比较而言，Decentraland 作为新兴元宇宙代表则在其平台规则中比较详细而明确地承认用户对其创制内容享有著作权等知识产权，即“用户对其创造的内容享有其上的所有权利、所有权和知识产权”〔27〕。

（三）元宇宙用户作品著作权归属的确定

《伯尔尼公约》的国民待遇原则足以确保元宇宙用户对其作品享有著作权。〔28〕世界上已经有 179 个国家加入《伯尔尼公约》，根据国民待遇原则，如果元宇宙用户属于成员国国民，其作品著作权自动在另一成员国获得同等保护；即使元宇宙用户不属于公约成员的国民或者属于无国籍人，只要在元宇宙上创作并发布作品，基于元宇宙的全球跨国同步运行的原理，该行为同样符合作品首次在成员国出版或者在一个非成员国和一个成员国同时出版的条件，其著作权也可以在该公约成员国获得同等保护。

在著作权归属上，世界各国的著作权法普遍提供两种规则：一般规则和特定作品的特殊规则。其中，《伯尔尼公约》明确了作品归属的一般规则，即作品著作权归属于作者，在作品之上署名的自然人推定为作者，但有相反证明的除外；即使作者采用假名，只要根据该假名可以准确识别作者身份，该推定同样成立。〔29〕在元宇宙中，用户通过元宇宙平台的账号创造的作品都会直接附属在这个账号之上，而且 Decentraland 等元宇宙平台本身是建立在区块链之上的，用户创制作品的著作权归属也可以借助区块链记载这一证据推定该用户所有人是作者，并借助区块链技术不可篡改的优点强化这一推定。不过，由于区块链只是将作品的哈希值而非作品本身记录在区块链之上，而且区块链平台并不审查作品上链前是否属于该特定区块链账户原始创作的作品，所以区块链记载也仅仅起到作品登记的证据效力，任何人有相反证据时，仍可以推翻前述权属推定。

相比之下，《伯尔尼公约》对于法人作品、职务作品、合作作品、委托作品、视听作品和演绎作品等特殊作品的著作权归属并未设定统一规则，留给成员国自行规定，〔30〕元宇宙的同一作品可能因不同国家对其归属的不同规定导致出现不同的著作权人，给该作品在元宇宙的跨国统一许可或转让等带来障碍。以其中最为复杂的视听作品为例，视听作品指的是一系列有伴音或无伴音的连续画面，包括电影、电视剧、短视频等形式，各国在规定其著作权归属时可能授予参与创作的自然人所有、制片人所有，或者自然人和制片人共同所有，也可以是自然人所有（即原始所有人）但默示转让给制片人（继受所有人），还可以是自然人所有但推定（可被推翻）转让给制片人。而且，各国的规定可能在不同时期出现变动，例如我国《著作权法》2020 年修订前采用电影作品和类电影作品概念，其著作权归属于制片人，编剧、导演、摄影、作词、作曲等作者享有署名权，但 2020 年修法时采用了视听作品的概念，其中电影作品、电视剧作品的著作权由制

〔26〕 Tilia Inc. User Terms of Service，available at https://www.tilia.io/legal/tos，last visited on Jul. 11，2022.

〔27〕 Decentraland Terms of Use，available at https://decentraland.org/terms/，last visited on Jul. 11，2022.

〔28〕 参见《伯尔尼公约》第 3 条、第 4 条。

〔29〕 参见《伯尔尼公约》第 15 条第 1 款。

〔30〕 参见《伯尔尼公约》第 14 条。

作者享有，可以单独决定电影作品的利用，编剧、导演、摄影、作词、作曲等作者享有署名权，但短视频等其他类型视听作品则由参与创作的主体约定其著作权归属。〔31〕

有鉴于此，《伯尔尼公约》第 14 条之二专门协调电影作品的著作权归属及著作权人的权利边界。首先，电影作品著作权归属原则上由被要求保护国的著作权法来决定归属，并且在该国内的电影作品利用则按照该国的规则确定；其次，如果被要求保护国著作权法承认参加电影作品制作的剧本作者、配乐作者、台词作者、电影主要导演之外的自然人（如摄影、副导演）属于著作权人，该国法律除非另有特别规定，应当默示承认这些作者不能反对对电影作品的复制、发行、公开表演、演奏、向公众有线传播、广播、公开传播、配制字幕和配音。尽管做了这样的协调，成员国的这些规定仅适用于成员国内部，仍然会出现同一电影作品在不同成员国有不同权利人的局面，仍然无法解决全球统一许可和转让的问题。一种可能的解决方案是，以最密切联系国的著作权法来确定这些特殊作品的著作权归属并由该权利人统一决定后续的利用，其中的最密切联系点可以体现为主要决定这些特殊作品的内容创作行为或者投资行为的实施地。

三、作品跨境同步利用的挑战

基于元宇宙在全球去中心化的同步运营，元宇宙中作品的利用因为涉及不同国家的不同著作权法，除了前述不同著作权归属带来的难题外，同一利用行为也可能涉及不同国家的不同具体著作权，这些权利的许可和转让都会给元宇宙作品全球跨境跨平台利用制造障碍。

（一）元宇宙利用涉及的具体著作权

元宇宙的全球去中心化运营表明它是一个公众中不特定成员可以自由访问并受现实法律规制的空间，那么，元宇宙用户创作完作品之后的利用行为都可以落入著作权法框架下具体权利控制范围，作品的许可和转让合同要协调不同国家的不同规定。

著作权主要分为人身权利和财产权利，人身权主要包括署名权、发表权、保护作品完整权，财产权利主要包括广义上的复制权、传播权和演绎权。在元宇宙中利用作品都要受到这些权利的控制。例如，用户利用元宇宙平台提供的工具创作完成作品之后，选择对外发布即公众可见，相当于行使了著作人身权中的发表权，而且发表权一经行使就用尽。又如，虚拟物品发布后向公众展示，让公众中的成员可以访问该作品，那么该行为就受传播权的控制。如果将虚拟物品铸造成 NFT 进行出售，其中铸造和发行可能涉及复制权、传播权。如果允许他人在自己作品之上继续创作可能涉及演绎权。值得注意的是，如果将不在元宇宙中创作的作品以 NFT 画框的形式展示在元宇宙空间内，〔32〕同样涉及作品的传播权。

然而，每个国家著作权法对人身权、复制权、传播权和演绎权的具体规定并不相同。例如，对公众可以在选定时间和地点获得作品的控制，在我国法规定为信息网络传播权，但在美国法则

〔31〕 参见《著作权法》（2010）第 15 条；《著作权法》（2020）第 17 条。

〔32〕 Decentraland 就允许注册用户这样做。用户只需要在虚拟土地上设置一道墙，在墙上就可以装一个展示 NFT 数字藏品的画框。然后就可以将 Decentraland 之外的 NFT 的 ID 和 NFT 合同地址复制到这个 NFT 画框中，这个 NFT 就可以在这个虚拟空间中展示出来。

可能受制于公开展示权（针对作品单个复制品或者视听作品中图片的单独展示）或者公开表演权（针对视听作品图片的连续性表演）。这就造成对全球同一行为的控制到底应当通过许可或者转让哪一个权利来实现的技术性问题。

（二）对元宇宙平台作品利用的全球授权模式

在元宇宙中作品的统一许可或转让更有利于著作权人进行作品管理和收益。一方面，虽然元宇宙未改变著作权法的地域性以及著作权的私权属性，著作权人对作品的利用可以选择各国的单独许可和转让，但著作权人这样做的同时也要背负根据单一国家著作权法确定交易的合同条款和价格所带来交易成本。这种单独授权模式很大程度上贬损了元宇宙去中心化全球运行的价值。另一方面，元宇宙全球统一实时运行意味着作者的版权市场是全球市场，所有潜在买家都可以同时参与交易甚至是竞价，从而让作者以最低成本实现利益最大化。在这里，有两大技术帮助著作权人实现作品全球统一管理，并以最低的成本实现利益最大化。一是智能合约，它是合约（交易规则）的代码（即计算机程序），可在区块链上运行，一旦触发合同生效的条件即可自动执行。因此，著作权人可以通过智能合约自动执行作品的交易和营收分配，省去了各国层层中间商或者著作权集体管理组织的代理环节和利益分流。二是谷歌浏览器等语言自动翻译技术，传统环境下的作品传播和交易可能存在不同国别有不同的语言和传播范围的局限，但是目前很多采用 NFT 形式开展的作品交易可以通过谷歌等浏览器实时进行作品内容和交易条件的翻译，〔33〕从而破除了过去的语言障碍。

实践中，元宇宙作品利用的主体主要有两大类，元宇宙平台和元宇宙用户。对于元宇宙平台的利用，著作权人往往不得不同意元宇宙平台制定的格式合同条款。其中，元宇宙平台根据其是否利用区块链技术可以分为中心化运营元宇宙和去中心化元宇宙，而中心化运营元宇宙是元宇宙的过渡形式。因此，《第二人生》这类中心化平台的平台规则往往要求用户对其创造作品的著作权提供宽泛的全球免费许可，“您同意授予一个全球、免费、可再许可、可再转让的，有关您上传、存储、发送、接收或者通过本服务而提供的任何内容的使用、复制、发行、演绎、展示等许可”〔34〕。在这里我们可以发现，该平台选择的许可规则已经超出了一国对作品利用应当明确具体许可的权利类型和一国地域范围之内的通常规则。〔35〕同时，考虑到元宇宙的全球运营以及各国著作权法对著作权具体权利的不同规定，该许可条款直接规定许可针对的是任何使用（并列举主要的利用形式，如复制、展示），而不指向具体权利的许可。此外，可再许可的要求也对未来多平台互联互通的利用预留了空间。

相比之下，利用区块链技术的去中心化元宇宙平台则遵守区块链尤其是公链的去中心化运行的特性，不对用户创制作品进行集中存储、审核和事前管理，也不直接调用用户的作品。〔36〕例如，基于以太坊区块链运作的 Decentraland 在其平台规则中规定，用户在该平台购买虚拟土地后可以在该土地之上自主创设任何内容（包括符合作品条件的内容），并且对其拥有绝对的控制权，

〔33〕 Decentraland 默认要求通过谷歌浏览器来进行翻译。

〔34〕 Art. 6. 3 of Tilia Inc. User Terms of Service.

〔35〕 例如我国《著作权法》第 26 条规定著作权许可使用合同应当包括许可使用的权利种类、许可使用的地域范围的形式要求等内容。

〔36〕 例如，Decentraland 对用户内容采用去中心化存储方式，用户计算机自行存储其创设的虚拟物品，平台服务器上仅仅存储可以调用该作品的区块链地址。参见前引〔4〕，Decentraland 书，第 9 页。

而未规定平台对用户作品的利用。〔37〕

（三）NFT 形式的作品利用授权

元宇宙中作品利用的主要市场来自其他用户的交易和后续使用，具体交易对象主要有两种，用于装扮化身的可穿戴虚拟装备和其他虚拟现实物品（包括外形上与现实世界物品类似或一致的虚拟物品和数字化的传统艺术品）。这两种交易主要通过 NFT 技术来实现交易对象的确认、跟踪和流转。〔38〕NFT 即不可替代代币或者非同质化代币（Non-Fungible-Tokens），指的是一种基于智能合约管理的具有不可分割、不可替代、可验证、可流通等特性的数据单元（合同地址，unit256代币标识），每一个代币标识都对应一个合同地址而可以代表对数字或者实物资产的所有权。〔39〕目前，NFT 主要指的是通过以太坊《ERC-721：NFT 智能合约标准》发行的 NFT，该标准定义了在以太坊智能合约上跟踪、流转 NFT 的应用接口规范。〔40〕每个 NFT 在 ERC-721 智能合约中都通过 unit256 数据（即元数据）而获得唯一标识（简称 Token ID），该标识在合同有效期内不得更改，并以“合同地址，unit256 代币标识”的形式成为特定资产在以太坊链上的全球唯一的标识符，用于指示该合同地址所有者对代表数字资产的标识拥有所有权，可以决定对该资产是否进行交易以及交易的条件。〔41〕

在 ERC-721 标准下铸造 NFT 时通常会涉及著作权控制的有关作品利用行为。第一步：将数字内容上传至网络服务器（可以是集中或者分散的服务器）可能涉及作品的复制。拥有以太坊钱包（钱包地址就是合同地址）的用户，通过某个以太坊应用平台（如 Opensea）将特定数字内容（如图片、视频、3D 模型等）上传至该平台的服务器，从而在该服务器上形成了有关该数字内容的复制品，并生成有关该内容的网络地址。如果数字内容构成作品，那么该上传行为构成作品复制行为，〔42〕至于是否会演变为传播行为则取决于 NFT 铸造者的下一步行为。

第二步：用户在设定该 NFT 交易规则时可能涉及提出有关作品许可或转让的要约或者创设事实上的追续权规则。在创制 NFT 时，铸造者可以选择在智能合约用户界面上描述该数字内容，如著作权人是谁，购买者获得该 NFT 的意义（如可以获赠一张带有创作者签名的作品复制品），以及转售该 NFT 时创作者可以获得的利益分成（不高于交易费的 10％），用户也可以选择不对这些内容进行描述，而只描述该数字内容是什么。这一步骤可能发生两个关键著作权行为。一是提出有关 NFT 交易的著作权许可或转让条件，只要该条件非常明确则可以构成要约（如包括了交易标的、交易价格和附带的著作权许可或转让约定），一旦买方同意该交易条件并点击确认交易则构成承诺，交易双方根据智能合约的自动执行即可达成有法律约束力的著作权许可或转让合

〔37〕 参见前引〔27〕。

〔38〕 See Decentraland Content Policy，available at https://decentraland.org/content/，last visited on Jul. 11，2022. 当然，在不依赖区块链技术的早期元宇宙平台如《第二人生》，则不必依赖 NFT 进行交易，而如同传统中心化组织管理下的交易。在该技术下的交易，玩家购买可穿戴等虚拟物品，如这些虚拟物品具有著作权，玩家仅仅获得了一份作品复制品的使用权，也未获得该复制品的所有权。

〔39〕 See EIP-721：Non-Fungible Token Standard，available at https://eips.ethereum.org/EIPS/eip-721，last visited on Jul. 11，2022.

〔40〕 参见前引〔39〕。

〔41〕 参见前引〔39〕。通常合同地址也就是创制该 NFT 的用户，即 NFT 原始所有人。

〔42〕 参见陶乾：《论数字作品非同质代币化交易的法律意涵》，载《东方法学》2022 年第 2 期。

同。不过，ERC-721 标准并不要求 NFT 铸造者作出有关作品著作权许可或转让方面的描述或约定，因为一旦描述就构成智能合约的一部分并在条件成就时自动执行合同条款。一方面，ERC-721 标准制定者并不想干预铸造者在这方面的自由，另一方面智能合约只保障计算机环境下合约的自动执行，而不保证现实世界作品的许可和转让的自动执行。

第二步的第二个关键行为是 NFT 铸造者一旦设定了 NFT 二次交易时交易费用返回给 NFT 铸造者的比例，则构成通过智能合约设定事实上的作品追续权规则。为了吸引艺术家采用以太坊上 NFT 这种新型应用，形成良好生态，部分 NFT 平台允许艺术家选择在智能合约中设定 NFT 二次交易利益分享比例（例如 Opensea 平台要求不超过 10%），在 NFT 二次交易时基于智能合约的自动执行产生类似法定追续权的效果。然而，这种做法并不满足法定追续权的三大要件。追续权指的是作家和作曲家对其艺术原作和原稿在二次交易时对二次交易价格享有一定比例的利益分配权。对此权利《伯尔尼公约》并未硬性规定，目前法国等 80 多个国家已有规定，我国不在此列。〔43〕追续权的第一要件是作品类型及载体限制，仅限于艺术作品的原作和原稿。NFT 涉及的往往是上传至 NFT 平台的作品复制件。第二个要件是对作品原件和原稿首次交易后二次公开商业化交易，私下交易不受该权的限制。NFT 二次交易会记录在区块链上，满足公开交易要求，因而可以满足该要件。三是二次交易利益分配的对象和比例由成员国法律确定，不能由当事人自行确定。〔44〕NFT 二次交易的利益分成则在平台最高限框架下由作者自行决定，不能代表国家意志。

第三步：发布 NFT 可能涉及作品的传播行为。完成前面两步，该 NFT 尚未对外发布也未被写入区块链。区块链上记录内容的算力成本和燃费（gas）都非常高，因此所记录的仅仅是交易摘要的哈希值和时间戳。铸造 NFT 本身只是对上传到网络服务器上的数字内容复制品的所在网址根据特定算法生成了唯一标识码，只有其他用户购买该 NFT 时才能完成交易，这时形成的交易摘要的哈希值才会上链记录。同时，考虑到防止恶意交易和激励矿工耗费算力对交易进行上链，NFT 铸造者在发布前往往被要求预付 NFT 交易上链的燃费。〔45〕只有支付足额燃费后，该 NFT 才会正式在 NFT 交易平台上发布，并在未来交易完成时上链。在 NFT 平台发布后，公众即可在选定时间和地点，通过 NFT 附带的网络地址或者哈希值全网搜索的形式，访问存储在网络服务器的作品。因此，发布 NFT 受传播权的控制，具体到我国则是信息网络传播权。〔46〕

第四步：交易 NFT 可能涉及作品利用的正式授权，但通常购买者仅通过交易获得了代表数字内容的唯一标识码，并未获得著作权法意义上的著作所有权。NFT 在 NFT 平台发布后，任何公众只要用其数字签名确认接受该 NFT 的出售价格和附带的智能合约并完成支付，双方就通过要约和承诺形成了交易合同，区块链则根据智能合约自动记载此次交易摘要的哈希值，相应地该 NFT 的数据单元（合同地址，unit256 代币标识）中的卖家合同地址就会替换为买家合同地址，买家据此持有了该 NFT。然而，购买者实际上仍然没有获得作品本身，而仅仅持有该作品在

〔43〕 参见李雨峰：《论追续权制度在我国的构建》，载《法律科学》2014 年第 1 期。

〔44〕 参见世界知识产权组织：《世界知识产权组织管理的版权及相关权条约指南以及版权及相关权术语汇编》，世界知识产权组织 2004 年版，第 67 页。

〔45〕 参见邹军等：《区块链技术指南》，机械工业出版社 2018 年版，第 44 页。

〔46〕 参见杭州互联网法院（2022）浙 0192 民初 1008 号民事判决书。

• 62 •

NFT 平台上对应的唯一标识码，也没有获得独家访问上链前存储在网络服务器上对应作品复制品的权利，因为该复制品为了后续 NFT 二次交易而仍存储在网络服务器上并供公众公开访问。〔47〕值得注意的是，鉴于发行权必须涉及作品有形载体所有权的转移，〔48〕卖家或者作者通过 NFT 交易也并非在行使发行权：一是因为 NFT 交易仅涉及作品数字化复制品的元数据（unit256代币标识）的持有者改变（合同地址发生变化），而并非作品原件或复制件所有权的改变；二是《ERC-721：NFT 智能合约标准》并不要求 NFT 平台或者 NFT 铸造者必须在智能合约中约定交易完成即将存储在 NFT 平台上的作品复制品发送一份给买方，买方因而不必然获得作品原件或者复制件，而通常获得访问 NFT 平台上作品复制件的权利。〔49〕

因此，元宇宙用户利用以太坊《ERC-721：NFT 智能合约标准》铸造 NFT 与其他用户交易时，假设这些 NFT 所指向的数字内容构成受著作权法保护的作品，用户通过 NFT 平台发布 NFT 相当于默示授予该平台在全球范围内的作品使用许可，〔50〕以供其存储一份复制品并在全球范围内公开展示该复制品；〔51〕同时默示授予购买 NFT 的用户个人在全球范围内的非商业性使用许可，以供购买者在全球根据自己选定的时间和地点访问该复制品，甚至使用该复制品（如将可穿戴物品穿搭在化身上），但购买者持有该作品复制品的全球唯一标识码本身跟著作权没有任何关系。不过，作者如果在铸造 NFT 时在标准智能合约之外作出其他著作权许可或者转让要约，〔52〕在购买者作出承诺并支付更大对价时，则与购买者达成相应的著作权许可或者转让合同。只要这类超出智能合约自动执行的合约部分符合法律的要求，完全可以通过法院加以强制执行。〔53〕

四、作品侵权救济的挑战

元宇宙用户在自行创制作品的过程中可能有三个场景会发生著作权侵权：一是将他人现实世界的作品复制到元宇宙中，如将他人的名画数字化后制作成元宇宙内的虚拟物品进行售卖；二是在元宇宙中对他人在元宇宙创作的作品进行复制，例如将他人在元宇宙创造的 3D 作品超出其著作权许可范围进行演绎或者商业性使用；三是将他人在元宇宙中的作品复制到现实世界，例如将他人的 3D 虚拟物品打印成平面图片印制在 T 恤上出售。在无授权的情况下使用他人作品即构成

〔47〕 当然，这里并不排除卖家通过智能合约对作品复制品作出其他专门安排，也不排除该 NFT 平台因为服务器故障或其他原因导致公众无法再次访问该作品复制品。

〔48〕 参见前引〔44〕，世界知识产权组织书，第 165 页；李明德、管育鹰、唐广良：《〈著作权法〉专家建议稿说明》，法律出版社 2012 年版，第 226 页。

〔49〕 在这个交易中，不排除卖家为买家提供其他承诺，如线下提供作品有形载体并附上签名，只有买家线下获得该作品有形载体时才会涉及发行权问题。对发行权的讨论，可参见前引〔42〕，陶乾文；杭州互联网法院（2022）浙 0192 民初 1008 号民事判决书。

〔50〕 国内一些公司为了满足国内的监管需求采用联盟链或者私链供用户铸造 NFT，此时的许可通常限于国内。参见杭州互联网法院（2022）浙 0192 民初 1008 号民事判决书。

〔51〕 参见前引〔42〕，陶乾文。

〔52〕 See Megan E. Noh，Sarah C. Odenkirk & Yayoi Shionoiri，GM! Time to Wake Up and Address Copyright and Other Legal Issues Impacting Visual Art NFTs，45（4）Columbia Journal of Law & the Arts，7（2022），available at SSRN：https://ssrn.com/abstract=4028116，last visited on Aug. 8，2022.

〔53〕 有关实践可以参见耐克公司旗下的 RTFKT 公司的 NFT 许可协议。See RTFKT，Digital Collectible Limited Commercial Use License Terms，available at https://rtfkt.com/legal-2A，last visited on Jul. 11，2022.

侵权，因而这些场景下的著作权侵权在侵权判断标准上跟现实世界没有差异，即首先确认原告是否享有著作权，然后判断被告行为是否落入著作权人专有权控制的范围。然而，元宇宙的去中心化运营却可能给著作权人维权带来挑战：一是司法管辖权的确定；二是准据法的确定；三是著作权停止侵权在区块链技术下的实现。

（一）司法管辖权的确定

基于元宇宙的全球去中心化运行，用户的账户采用区块链钱包（即私钥管理软件），用户的身份是匿名并且对平台而言通常也是匿名的，况且利用区块链的元宇宙平台管理者往往是去中心化组织（例如 DAO）。那么，一旦发生著作权侵权，著作权人应当向哪里的法院起诉这些侵权人，法院又是否有权审理发生在他国的侵权行为？例如，拥有 A 国国籍的张三复制了拥有 B 国国籍的李四的作品，并利用王五在 C 国运营的 NFT 平台铸造了 NFT，并利用在 D 国设立运营的元宇宙平台 Decentraland 中的 NFT 画框将该 NFT 植入 Decentraland，那么全球公众可以通过上述 NFT 平台或者 Decentraland 访问到上述作品。这时，李四作为著作权人面对这种涉外侵权纠纷是选择在 ABCD 四个国家同时起诉，还是选择在某个国家起诉张三要求对在全球范围内造成的损害结果承担责任，上述主张又能否得到法院的支持，就成为问题。

《伯尔尼公约》第 5 条规定，作者享有的具体著作权、保护的程度以及为保护作者权利而向其提供的救济方法完全由被要求给予保护的国家的法律规定。WIPO 在解释该条款时只强调被要求给予保护国著作权法的决定事项并不延及著作权的许可和转让等合同问题，并未明确涉外著作权案件的管辖权。〔54〕对此，国际著名版权法学家山姆·里基森、简·金斯伯格指出，涉外著作权侵权案件的司法管辖权由各国自行规定。〔55〕然而，各国对涉外案件的司法管辖权规定并不统一，可能采取属人管辖权或者对事管辖权，或者二者兼有。其中，前者的联结点是被告所在地，包括了国籍地和经常居住地。后者的联结点多是侵权行为地、侵权结果地、被告可供扣押财产所在地。例如，我国《民事诉讼法》第 272 条规定，因财产权益造成的涉外纠纷，对在中华人民共和国领域内没有住所的被告提起的诉讼，可以由诉讼标的物所在地、可供扣押财产所在地、侵权行为地或者代表机构住所地人民法院管辖。〔56〕

各国不同的司法管辖权规定可能带来的重要影响除了诉讼的成本之外，还有法院有权对原告提出的哪些诉求进行审理，最终影响原告能否通过单一诉讼获得充分救济。通常而言，限于著作权法的地域性，如果法院实施管辖的联结点是侵权结果发生地，那么法院的审理权限也限于该国境内的损害，无权审理发生在他国的损害；当实施管辖的联结点是侵权行为地或者被告所在地时，法院仍不能通盘考虑发生在其他国家的侵权，原告需对在其他国家产生的损害结果发起单独诉讼。〔57〕对

〔54〕 参见前引〔44〕，世界知识产权组织书，第 31 页。

〔55〕 参见〔澳〕山姆·里基森、〔美〕简·金斯伯格：《国际版权与邻接权——伯尔尼公约及公约以外的新发展》，郭寿康等译，中国人民大学出版社 2016 年版，第 1145 页。

〔56〕 对于其中涉及信息网络传播权的侵权行为地，《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》第 15 条规定，侵权行为地包括实施被诉侵权行为的网络服务器、计算机终端等设备所在地，但侵权行为地和被告住所地均难以确定或者在境外的，原告发现侵权内容的计算机终端等设备所在地可以视为侵权行为地。

〔57〕 例如，在普通法系国家，这一规则被称为属地诉讼而不是追身诉讼。See Paul Goldstein & Bernt Hugenholtz, International Copyright: Principles, Law, and Practice, Oxford University Press, 2013, pp. 118 - 120.

此问题，欧盟《布鲁塞尔条例》允许侵权实施地或者被告住所地法院审理跨越多国的著作权侵权案件。〔58〕然而，我国对此问题尚未明确规定，未来我国法院在审理元宇宙著作权侵权案件时就要对此作出选择。目前而言，我国采用类似欧盟的做法更为可取，一方面国际上有这样的先例，另一方面能最大化保护著作权人的合法利益。

此外，如果多国法院依据本国法都有权管辖时，而且原被告就同一侵权行为在多国起诉时，那么各国诉讼之间应当如何处理，是最先受理法院先行审理、其他国家法院应等待先行审理判决后才能审理，还是不受先行审理法院的影响？对此，各国做法也不统一，目前中国法院〔59〕和美国法院认为不受影响，欧盟国家遵守《布鲁塞尔条约》则要等待先行审理法院的结果。〔60〕因此，元宇宙案件中原告在A国提起侵权之诉，而被告在B国提起确认不侵权之诉时，两诉之间的关系受制于这两个国家之间是否存在管辖权的条约，如果缺少则完全取决于这两个国家的各自规定。〔61〕对此，可能的理想解决方案是鼓励当事人在双方协商确定的法院进行诉讼，从而避免陷入多国竞争诉讼的泥潭。

（二）准据法的确定

按照《伯尔尼公约》第5条规定，一旦著作权人选择在某国提起著作权侵权之诉，那么其作品著作权的具体权利内容、保护的程度以及救济方法都归该国法律来确定。同时，《伯尔尼公约》仅规定了著作权保护的最低要求，各国在作者享有的著作权、保护的期限、行政救济或司法救济的单轨保护还是双规保护、损害赔偿是否包括惩罚性赔偿及其计算方法等方面都各不相同。例如，德国法规定公开提供权控制作品的网络交互式传播，作品保护期持续到自然人作者死后七十年，但并未规定著作权侵权的惩罚性赔偿。相比之下，中国法规定信息网络传播权控制作品的交互式传播，作品保护期仅持续到自然人作者死后五十年，但提供了一至五倍的惩罚性赔偿。

由此，各国的规定可能导致著作权人获得的保护在结果上有违国民待遇原则，于是《伯尔尼公约》对第5条又做出了例外规定。〔62〕首先，各国可以自主决定对实用艺术品以及工业品平面和立体设计提供专门法保护或者著作权法保护（但保护期不得少于25年），如果起源国和被要求保护国都仅提供专门法保护，则按照被要求保护国的专门法保护，如果被要求保护国仅提供著作权法保护，则按照作品提供保护。〔63〕因此，如果元宇宙用户将现实世界的实用艺术品及工业品平面和立体设计复制到元宇宙中，要遵守这一例外规定。

其次，被要求保护国对作品的保护期限如果超过作品起源国，仍以起源国的保护期限为准。〔64〕其中，关于何为作品起源国：对于首次在《伯尔尼公约》成员国出版的作品，以该国家

〔58〕 参见前引〔55〕，山姆·里基森、简·金斯伯格书，第1146－1148页。

〔59〕 参见《最高人民法院关于适用〈中华人民共和国民事诉讼法〉的解释》第533条；张鹏：《跨境知识产权侵权纠纷的民事诉讼管辖规则研究》，载《知识产权》2022年第1期。

〔60〕 参见前引〔57〕，Paul Goldstein、Bernt Hugenholtz书，第125页。

〔61〕 类似问题在标准必要专利全球诉讼中尤为明显，各国对标准必要专利的FRAND许可原则的解释不一，而且还可能通过禁诉令的形式要求当事人不得在全球其他法院就同一问题进行起诉。参见前引〔59〕，张鹏文。

〔62〕 参见前引〔55〕，山姆·里基森、简·金斯伯格书，第1150页。

〔63〕 参见《伯尔尼公约》第2条第7款。

〔64〕 参见《伯尔尼公约》第7条第8款。

为起源国；对于在分别给予不同保护期的几个本同盟成员国同时出版的作品，以立法给予最短保护期的国家为起源国。〔65〕在元宇宙全球同步运行的情况下，元宇宙内创作的作品的保护期往往以《伯尔尼公约》成员国中给予最短保护期的国家为起源国。不过，在涉外诉讼中其保护期仍然可以按被要求保护国提供的更长保护期计算。

最后，对于追续权的保护，被要求保护国不提供追续权保护的，或者被要求保护国提供追续权保护但作者国籍国不提供追续权保护的，那么该追续权主张无法得到被要求保护国法院的支持；作者国籍国和被要求保护国同时提供追续权保护的，以被要求保护国为准提供保护。〔66〕因此，元宇宙用户如果选用 NFT 来出售作品，并且在智能合约中设定了二次销售的利益分享比例，那么借助智能合约的自动执行，铸造 NFT 的用户可以获得这些分成，不论被要求保护国和作者国籍国是否提供追续权保护。然而，如果该用户并非著作权人，著作权人起诉时，在被要求保护国提供追续权保护但作者国籍国不提供追续权保护的情况下，法院不保护著作权人的追续权诉求，但这里不排除法院将其作为侵权人获利计入其他侵权的损害赔偿额。此外，在被要求保护国提供的追续权二次交易利益分享比例高于作者国籍国保护程度且高于侵权人在智能合约中设定的比例时，著作权人应当获得的追续权利益要比智能合约自动执行的还要高。

因此，元宇宙本身对著作权侵权的准据法确定本身并未提出挑战，但对当事人维权设置了难题：当事人不仅要考虑哪国是否有管辖权、是否最适合管辖等程序问题，更要结合具体侵权情况考虑该国实体法是否更有利于保护自己的利益。

（三）共同侵权的被告问题

在元宇宙环境下的著作权侵权涉及元宇宙平台和侵权用户的责任问题，然而元宇宙依靠区块链去中心化运行会带来两个问题：一是缺乏内容集中存储和统一控制的中心化平台，平台的管理组织通常是去中心化运行的 DAO 组织；二是在区块链上开发元宇宙并不要求用户在平台中提供身份信息注册才能登录元宇宙，相反该元宇宙平台往往允许拥有相应区块链账户的用户直接登录，此时元宇宙平台也不直接掌握用户的身份信息。那么，著作权人维权时应当如何确定和选择所要起诉的被告？

对此，我们仍然需要结合被要求保护国有关共同侵权或者间接侵权规则来确定起诉的主体。各国这些实体法通常直接适用于著作权领域，各国在具体规则上仍然存在差异。例如，美国的间接侵权规则主要是法院形成的判例法，包括了帮助侵权、替代侵权和引诱侵权，并在一系列涉及作品 P2P 共享的案件中引入著作权侵权领域，这些判例的特点是原告著作权人可以仅仅起诉提供共享技术的平台并要求其承担间接侵权责任，而无须起诉直接侵权人。那么，著作权人选择在美国起诉著作权侵权时，就可以不再单独考虑起诉直接侵权的用户，而可以选择起诉 DAO 组织承担间接侵权责任。虽然 DAO 组织不实际存储所有用户上传的内容，但它仍然是这个平台运行规则的实际制定者（可以通过成员投票改变平台运行规则，如加入作品上传的审查要求）并拥有财产（通常是信托财产）。〔67〕

〔65〕 参见《伯尔尼公约》第 5 条第 4 款。

〔66〕 参见《伯尔尼公约》第 14 条之三。

〔67〕 参见前引〔4〕，Decentraland 书，第 5 - 14 页。

相比之下，我国法下共同侵权规则有三个特点：一是起初《民法通则》虽然规定了帮助侵权条款，但法院在适用时往往要求原告同时起诉直接侵权人和帮助侵权的平台，否则以不能查明案件事实为由不予受理或者驳回起诉，〔68〕后来《侵权责任法》和《民法典》的网络侵权条款都直接规定了帮助侵权的平台因为自己的行为要独立承担侵权扩大责任，所以元宇宙平台也可以作为帮助侵权人被单独起诉；〔69〕二是我国没有对应的替代侵权，最高人民法院在相关著作权侵权司法解释中指出平台直接从直接侵权中获利的要承担更高的注意义务；〔70〕三是我国最高人民法院在相关著作权司法实践中也明确了引诱侵权，元宇宙平台以言语、推介技术支持、奖励积分等方式诱导、鼓励用户实施侵害信息网络传播权行为的，也可以被单独起诉要求承担责任。〔71〕由此可见，各国的共同侵权规则不仅存在差异，而且各自可能还在不断发展变化，著作权人在维权时要进一步考虑准据法中的共同侵权或者间接侵权规则，最终确定所要起诉的被告及其承担的具体侵权责任。

（四）停止侵权责任的承担方式

元宇宙的去中心化运行往往依赖区块链技术，该技术的分布式记账导致当事人无法篡改有关作品的交易记录，因而可以通过交易价格与区块链交易记账的燃费和中介费的差价来计算出交易的获利，以此确定损害赔偿的数额，从而让著作权人更容易获得准确的损害赔偿。

然而，区块链技术导致交易记录不可篡改和智能合约的自动执行也给著作权的停止侵权带来了一定的挑战，如可能导致侵权状态自动持续下去。对此，为了防止 NFT 交易的持续，国内法院在第一起 NFT 案件中认为，“（NFT）平台可将该侵权 NFT 数字作品在区块链上予以断开并打入地址黑洞以达到停止侵权的法律效果”〔72〕。其中，黑洞地址指的是丢了私钥或者无法确定其私钥的地址，〔73〕而地址就是用户账户，即用户在区块链所用加密技术中分配的公钥，缺少了对应的唯一私钥用户就无法再操控该账户，由此 NFT 交易到这些地址后就像进入黑洞一样无法逃逸，尽管该 NFT 仍然存在但无法进行后续交易。〔74〕同时，由于用户在铸造 NFT 时将作品复制品上传于 NFT 平台并形成了该复制品的网络地址，任何人全网搜索该地址即可访问到该复制品。因此，法院认为在区块链上对数字作品的网络地址予以断开并将该 NFT 打入黑洞地址可以实现停止侵权的效果。〔75〕

对于法院的上述做法，我们应当回归到停止侵权的责任形式来评价。我国《著作权法》第 52 条规定停止侵权的责任形式是停止侵害，针对的是侵权人实施的侵害行为已经发生并且仍在继续的，〔76〕内容上不包括《民法典》第 1167 条规定的排除妨碍和消除危险这两种预防性责任形式。其中，排除妨碍适用的前提是侵权人实施的行为使他人无法行使或者不能正常行使人身、财产权

〔68〕 参见郑成思：《侵权责任、损害赔偿责任与知识产权保护》，载《环球法律评论》2003 年冬季号。

〔69〕 在国内第一起 NFT 案中，原告就仅起诉了 NFT 平台，而未起诉铸建涉案 NFT 的用户。参见杭州互联网法院（2022）浙 0192 民初 1008 号民事判决书。

〔70〕 参见《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》第 11 条。

〔71〕 参见《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》第 7 条。

〔72〕 杭州互联网法院（2022）浙 0192 民初 1008 号民事判决书。

〔73〕 以太坊官方黑洞地址为：0x0000000000000000000000000000000000000dEaD。See Christian Heidorn，How to Burn NFT on OpenSea in 4 Easy Steps，available at https://tokenizedhq.com/how-to-burn-nft-on-opensea/，last visited on Jul. 11，2022.

〔74〕 参见前引〔52〕，Megan E. Noh 文，第 14 页。

〔75〕 参见杭州互联网法院（2022）浙 0192 民初 1008 号民事判决书。

〔76〕 参见王利明主编：《中国民法典评注：侵权责任编》，人民法院出版社 2021 年版，第 39－41 页。

· 67 ·

益，〔77〕然而著作权的客体作品是非物质性或者非竞争性的，侵权人占有或以其他方式利用作品复制品并不妨碍著作权人行使著作权（如将作品许可他人使用），故著作权侵权不适用排除妨碍。消除危险是指负有责任的人支配下的物对他人人身和财产安全构成威胁，或者存在侵害他人人身或财产现实可能性的情况下，受到威胁的人有权请求消除这种危险，〔78〕然而如果他人仅仅持有一份作品复制品但未公开传播往往受隐私权或者著作权合理使用制度（如个人使用）的保护，并不必然威胁到著作权人的利益。在 NFT 侵权场景下，侵权行为首先表现为 NFT 平台用户未经许可将他人作品上传至 NFT 平台并生成一份复制品，这构成侵害复制权；其次，借助 NFT 平台的服务自动生成有关该作品复制品可公开访问的网络地址，该地址转化为 NFT 智能合约下的 unit256 代币标识并在后续交易完成时被写入区块链，而且任何人知悉或者持有作品复制件的网络地址或者其对应代币标识都可以访问该作品，这构成侵害我国法下的信息网络传播权。在这个过程中，用户是复制权和信息网络传播权直接侵权人，NFT 平台是帮助侵权人，但在该案中权利人仅向平台主张停止侵害，因此法院只要判令平台删除用户上传的侵权内容或者断开侵权链接即可。侵权用户持有 NFT 仅仅持有了侵权作品的网络访问地址并不等同于向公众提供侵权内容，一旦 NFT 平台断开了侵权链接，任何人持有的网络地址将不再能够访问涉案作品，著作权人停止侵害的诉求就可以满足，至于侵权用户继续交易 NFT，本质上并不会侵害著作权，〔79〕似乎造成了未来可能侵害著作权人的危险而需要请求消除危险，但著作权侵权不适用消除危险。况且，在以太坊等公链技术之下，NFT 平台通常无权操纵用户账户使涉案 NFT 与黑洞地址发生交易。当然，在该案中，NFT 平台刚好利用的是联盟链，平台在技术上仍能够操纵用户，但这对联盟链的声誉实质上是一种伤害。

回归到元宇宙中 NFT 的停止侵权问题，元宇宙平台理论上采用公链技术，平台无法直接操纵用户账户使之与黑洞地址发生交易。而且，元宇宙平台中的用户内容往往存储在用户自己的电脑终端或者其他分散的节点，只有用户删除该终端上的侵权内容或者将侵权内容移出共享文件才可以实现停止侵害，即侵权内容不再被访问。因此，著作权人主张停止侵害的应当起诉侵权的元宇宙用户。值得注意的是，采用公链技术的元宇宙平台往往不要求用户使用真名，也不要求注册时提供真实身份信息，甚至可能不要求用户注册而直接使用其公链钱包账户登录元宇宙平台，因此用户真实身份往往难以确定。〔80〕如果该侵权用户不主动表明身份就很可能逍遥法外，〔81〕这时的停止侵害可能得通过改变区块链共识机制来实现。然而，共识机制是区块链运行的重大机制，需要大多数节点同意才能修改共识机制，因此修改共识机制的成本与某个作品著作权侵权损失相比完全不合比例，采用这种方法来实现停止侵权不具有操作性。〔82〕例如，在以太坊 the DAO 事件中，黑客攻击 the DAO 项目将价值 6000 万美元的 360 多万以太币转走，为了解决这次危

〔77〕 参见前引〔76〕，王利明主编书，第 41－42 页。

〔78〕 参见前引〔76〕，王利明主编书，第 42－44 页。

〔79〕 这时可能构成欺诈。

〔80〕 扎克伯格希望建立的元宇宙就主张用户采用与真实身份相一致的化身，包括化身的名字和外形。这就容易将用户的行为纳入法律的监管。此外，我国《区块链信息服务管理规定》第 8 条也要求区块链服务提供商对用户进行身份认证。

〔81〕 参见前引〔52〕，Megan E. Noh 文，第 14 页。

〔82〕 这种技术上的无解或者高成本解决方案，法律上也很难处理，除非从一开始就禁止使用公链或者强制要求公链进行实名化，但这相当于因噎废食。

机，以太坊创始人维塔利（Vitalik）通过改变共识机制的形式来追回部分被盗资金。〔83〕通常情况下著作权侵权损失达不到这个数额，而且修改共识机制也会对区块链的声誉造成重大损失。

五、结　论

打造元宇宙的目的不是平台集权式开发内容让用户娱乐，而是解放人们的创造力，让用户可以自由在虚拟现实空间中自由创作，并通过作品的分享与交易获得其他用户认可的声誉乃至经济回报，从而进一步激发用户在元宇宙中创作更多作品，〔84〕推进人类“向内”发展。〔85〕要实现这样的目的，元宇宙开发平台通过区块链提供用户创作的工具、社交的媒介和作品交易变现的经济体。鉴于这种虚拟与现实的交互，现实世界的法律应当适用于元宇宙，且不因元宇宙开发者意志而转移，包括元宇宙中的作品创作完成自动产生著作权，作品的利用应当获得著作权人的授权，未获得授权的使用构成著作权侵权等。而且，元宇宙借助区块链这种去中心化的分布式记账技术得到了前所未有的发展。借助区块链上运行的智能合约和 NFT 技术，用户可以对创作的作品在不依靠中间商的前提下完成交易并获得经济回报，实现了著作权制度设计者们梦寐以求的愿景——作品目标受众与作者的直接市场化连接。〔86〕不过，元宇宙的去中心化全球运行，也为作品的著作权归属、全球跨国许可或转让、著作权侵权救济带来一定的挑战，但通过对著作权的基本原理、《伯尔尼公约》等规则的适当解释以及技术解决方案，仍然可以妥当解决这些新型问题，尚不至于说元宇宙会颠覆传统著作权法。

Abstract：Metaverse is a decentralized virtual reality world that spans multiple jurisdictions. It provides users around the world tools to create copyrightable virtual objects and to trade them, thus build an environment for them to live a life by creating. However, the decentralized and cross-border operation of metaverse will bring a series of challenges to the territoriality of copyright legal system, creating legal uncertainty to the works' copyright ownership, specific copyright and degree of protection, utilization and tort relief. Anyway, by combining the scientific explanation of the basic principle of copyright rules, private international law, and technical solutions, those challenges could still be properly solved.

Key Words：metaverse, copyright, NFT

（责任编辑：殷秋实　赵建蕊）

〔83〕 参见伍旭川、刘学：《The DAO 被攻击事件分析与思考》，载《金融纵横》2016 年第 7 期。

〔84〕 参见邓建鹏：《元宇宙及其未来的规则治理》，载《人民论坛》2022 年第 7 期。

〔85〕 即向虚拟现实世界发展，相对于人类向外太空的发展而言。

〔86〕 参见〔美〕保罗·戈斯汀：《著作权之道》，金海军译，北京大学出版社 2008 年版，第 28 页。

财经法学 No. 5，2022
pp. 70 - 80

NFT 交易模式下的著作权保护及平台责任

王江桥*

内容提要：近年来，NFT 交易作为一种新兴的商业模式在快速发展的同时，亦对当前法律秩序带来挑战，产生了一系列新型法律问题。如何规制 NFT 市场，明确相关主体责任边界，依法保护各方主体的合法权益，从而引导 NFT 市场健康有序发展亦具有紧迫性。有必要从司法案例中反映的著作权问题出发，针对 NFT 模式下行为法律属性、NFT 交易平台的责任边界、数字作品是否适用权利用尽原则、侵权责任承担方式等新型法律问题进行分析研究。NFT 数字作品交易并非著作权法上的发行，应纳入信息网络传播权控制范畴；NFT 交易平台属于一种新型网络服务提供者，综合 NFT 数字作品的法律属性、NFT 交易模式、技术特点、平台控制能力、营利模式等多种因素，其应当承担较高的注意义务；NFT 侵权责任承担方式应当结合区块链技术特点予以合理确定。

关键词：NFT　信息网络传播　平台责任　侵权不停止

一、问题提出

近年来，NFT 交易作为一种新兴的商业模式得以快速发展，特别是 2021 年以来，我国相关行业对 NFT 的关注度急速升温。据不完全统计，腾讯、蚂蚁金服等一百多家企业纷纷推出各自的 NFT 发行平台。头豹研究院以阿里蚂蚁链销售额为基础，结合腾讯科技、Nonfungible 数据分析认为我国 NFT 市场在未来 5 年增长率约为 150%，市值有望达到近三十亿元。国外仅 Opensea 平台 2021 年的交易额就达到了 140 亿美元。〔1〕NFT 交易快速发展的同时亦带来了一系列新的法律问题，比如 NFT 模式下行为法律属性、NFT 交易平台的责任边界、数字作品是否适用权利穷

* 王江桥，杭州互联网法院副院长、三级高级法官。

〔1〕 参见头豹研究院：《2021 年中国 NFT 平台研究院报告》，第 19 页，载 https://pdf.dfcfw.com/pdf/H3_AP202202081545653782_1.pdf?1644314982000.pdf，最后访问时间：2022 年 8 月 5 日。

竭原则以及侵权责任承担方式等等，这无疑对当前法律秩序带来了新的挑战。目前相关法律规定尚属空白，相关理论界也鲜有深入研究。面对 NFT 交易引发的纠纷案件，司法并不能拒绝裁判，即使法律没有规定也不例外。法官或者运用法律解释方法，或者运用类推适用、目的性扩张等法律漏洞填补方法以及不确定性概念的价值补充方法、利益衡量方法来“发展”规则，为新的社会行为提供规则引导。〔2〕正如丹宁勋爵所言“法官不可以改变法律织物的编制材料，但是他可以也应该把皱熨熨平”〔3〕。2022 年 4 月 20 日，杭州互联网法院宣判了“NFT 侵权第一案”（以下简称 NFT 案），首次对 NFT 交易模式下的相关法律问题进行了分析和探索。〔4〕作为此案审理的参与者，现结合该案涉及的法律问题，从著作权保护角度就如何确定 NFT 交易模式下的行为属性、NFT 交易平台的责任边界以及侵权责任承担三个方面做一梳理和分析。

二、NFT 交易模式下的行为性质

（一）NFT 与 NFT 数字作品

NFT，是英文 non-fungible token 的简称，中文翻译包括“非同质化代币”“非同质化通证”“非同质化权益凭证”，是一种基于区块链技术而产生的不可复制、篡改、分割的加密数字权益证明。NFT 具体表现为通过区块链、智能合约等技术手段将数字内容确定为特定的交易对象，形成唯一对应关系，从而使其具有一定的交易价值，并作为特定客体实现在 NFT 交易平台进行交易流转。从外在表现形式来看，NFT 表现为区块链上一组加盖时间戳的元数据，〔5〕其与存储在 NFT 交易平台上的某个数字文件具有唯一的指向性，对应为一串独一无二的元数据库。该组元数据显示为存储特定数字内容的具体网址链接或者一组哈希值，点击链接或使用哈希值进行检索，就能够访问被存储的特定数字内容。〔6〕NFT 作为区块链下的一个新兴应用场景，一旦 NFT 被铸造，它就已经在区块链上以加密方式发布，使得 NFT 无法更改。同时，智能合约代码定义了 NFT 购买条件等规则，将促使并记录发生的所有 NFT 交易，并在满足其条件时自行执行 NFT 所有权转让。NFT 利用区块链技术记录并验证真实性，能够记录 NFT 数字内容的初始发行者、发行日期以及未来的每一次流转信息，做到全流程记录，区块链上所有节点同步予以见证，可确保数字内容公开透明、安全可信。NFT 本质是权利凭证而非权利，是一种特殊的具有稀缺性的链上数字资产，通过智能合约来实现其权利的转移，并通过区块链来记录权利转让的整个过程。〔7〕

NFT 数字作品属于典型的 NFT 数字资产，系将数字作品上传 NFT 交易平台并铸造 NFT 后再进行流通的数字内容。笔者认为，当一件数字作品以 NFT 形式存在于交易平台上时，由于数字作品数量的限量性和区块链节点之间的信任和共识机制，从而产生“特定性”“稀缺性”“价值

〔2〕 参见李占国：《网络社会司法治理的实践探索与前景展望》，载《中国法学》2020 年第 6 期。

〔3〕 丹宁勋爵：《法官绝不可以改变法律织物的纺织材料，但是他可以也应该把皱折烫平》，载 http://oppo.yidianzixun.com/article/0KUm3sQh? appid=oppobrowser&s=oppobrowser，最后访问时间：2022 年 8 月 5 日。

〔4〕 参见杭州互联网法院（2022）浙 0192 民初 1008 号民事判决书。

〔5〕 参见陶乾：《论数字作品非同质化代币化交易的法律内涵》，载《东方法学》2022 年第 2 期。

〔6〕 参见前引〔5〕，陶乾文。

〔7〕 参见陈吉栋：《超越元宇宙的法律想象：数字身份、NFT 与多元规制》，载《法治研究》2022 年第 3 期。

· 71 ·

性”等效果。NFT 数字作品以数据代码形式存在于虚拟空间且具备价值属性时，已具有数字商品属性；同时其亦具备一定的独立性、特定性和支配性，符合虚拟财产的基本特征，应属于虚拟财产范畴。当然，虽然 NFT 数字作品交易双方形式上呈现的是所有权人的变更，但我国《民法典》中物权编在定义所有权时，将其规定为“所有权人对自己的不动产或者动产，依法享有占有、使用、收益和处分的权利”。可见，虚拟财产并不属于上述法律规定的动产或不动产范畴，自然不存在所有权一说。

因此，NFT 数字作品交易并非实质意义上的所有权转让，而是一种数字资产（虚拟财产）转让。我国《民法典》第 127 条首次对虚拟财产的保护作出了规定，但对其法律性质并未予以明确，只是进行了宣示性或指引性规定。对于虚拟财产的法律属性，当前理论界与司法界存在物权说、债权说、知识产权说、新型财产权利等不同观点，但主流观点认为虚拟财产具有财产性利益，可以作为一种财产性权益予以保护。故此，NFT 数字作品交易中转让的对象本质上是一种受法律保护的财产性权益而非财产权利。换言之，NFT 数字作品被特定化为一个具体的“数字商品（资产）”后，呈现出一定的投资和收藏价值属性，并具有受法律保护的财产权益。NFT 交易本质上属于以数字化内容为交易对象的转让关系，购买者所获得的并非对一项数字财产的使用许可，亦非知识产权的转让或许可，而是一项财产性权益。因 NFT 数字作品购买者无法直接获得该数字作品，其享有的权利实际上主要表现为“所有权身份”和二次交易时的支配权。诚如“澎湃新闻社”专栏作家李奥尼德·波尔席斯基所言，NFT 购买方在多数情况下不过“是实施一个令人厌烦的摆显权”〔8〕。

（二）NFT 数字作品交易的行为属性

NFT 数字作品交易流程通常涉及铸造、上链、出售等环节。首先，从 NFT 数字作品的铸造流程来看，须将作品上传到 NFT 交易平台，故此时上传者终端设备中存储的数字作品被同步复制到网络服务器。其次，从 NFT 数字作品的上链环节来看，系在 NFT 交易平台上以出售为目的呈现该 NFT 数字作品，在作品被呈现的情况下，该展示行为使公众可以在选定的时间和地点获得作品。再次，从 NFT 数字作品的出售环节来看，由于 NFT 数字作品的交易条件及交易过程采用了智能合约技术，整个交易过程由智能合约中嵌入的“自动执行”代码触发完成。故当 NFT 交易平台注册用户通过数字钱包支付对价和服务费后，即刻成为平台上公开显示的该 NFT 数字作品的所有者。下面就 NFT 交易模式下的上述行为是否属于著作权法上的“复制”“信息网络传播”“发行”，以及是否适用“权利穷竭原则”等问题进行分析。

1. 是否属于著作权法上的“复制”

复制行为包括广义上的“复制”和狭义上的“复制”，前者可以理解为“再现作品”的行为，包括表演、广播、放映、改编等行为都可以被称为对作品的“复制”；后者仅指以特定方式对作品“再现”才是复制行为。〔9〕当前大多数国家的著作权法采用的是狭义上的复制行为定义。《中华人民共和国著作权法》（以下简称《著作权法》）第 10 条第 1 款第 5 项规定：“复制权，即以

〔8〕 Leonid Bershidsky, NFT Art Is All About the Hype, March 4, 2021, available at https://www.Bloomberg.com/opinion/articles/2021-03-04/the-nft-phenomenon-is-for-real, last visited on Aug. 5, 2022.

〔9〕 参见王迁：《知识产权法教程》，中国人民大学出版社 2021 年版，第 163 页。

印刷、复印、拓印、录音、录像、翻录、翻拍、数字化等方式将作品制作成一份或者多份的权利。”可见，我国著作权法上的复制权所控制的复制行为应当满足以下两个要件：一是该行为应当在有形物质载体（有体物）之上再现作品；二是该行为应当使作品被相对稳定和持久地“固定”在有形物质载体上之上，形成作品的有形复制件。〔10〕这里所指的复制件应当是产生新的复制件，即增加复制件的数量。当一件作品开始铸造 NFT 时，铸造者首先须按照平台要求上传作品，此时该作品的复制件已同步保存于平台网络服务器中。这种以数字化等方式将作品制作成一份的形式，一方面可以形成稳定的存储作品信息，另一方面亦形成了一个可以相对稳定、持久固定作品信息的有形物质载体，同时也具备作为信息源向其他载体进行信息传播的能力。因此，一件作品的铸造行为包含了著作权法所规制的复制行为。虽然上述复制行为的目的并非向他人提供作品复制件，但该复制件中的作品并未被后来的作品所替代，而是一种永久性的固定，因此，该行为亦并非临时复制。笔者认为，数字作品的铸造行为应属于复制权所控制范畴，其行为亦侵害了复制权。但因该复制是网络传播的一个必备步骤，其目的在于以互联网方式向社会公众提供作品，故复制本身给权利人造成的损害已经被信息网络传播给权利人造成的损害后果所吸收，〔11〕理应无需单独对此予以评价。当前司法实务中亦普遍采取此种做法，在认定构成信息网络传播权侵权的同时不再就复制行为进行评判。

2. 是否属于著作权法中的“信息网络传播”

信息网络传播权是随着互联网的迅速发展而产生，其目的是为了加强作品在互联网交互式传播中的著作权保护。《著作权法》第 10 条第 1 款第 12 项规定：“信息网络传播权，即以有线或者无线方式向公众提供作品，使公众可以在选定的时间和地点获得作品的权利。”据此，我国著作权法上的信息网络传播权所控制的信息网络传播行为应当具备以下条件：一是从作品使用的方式来看，该行为应当通过信息网络向公众提供作品；二是从效果来看，能够使公众在其选定的时间和地点获得作品。由于 NFT 数字作品通过铸造上链后，该数字作品系直接置于开放的网络服务器上进行交易，交易对象为不特定公众，且公众可以在选定的时间和地点获得 NFT 数字作品，故 NFT 数字作品上链交易行为符合信息网络传播行为的特征。铸造者未经许可通过 NFT 交易平台上链交易 NFT 数字作品的行为，应认定为侵害作品的信息网络传播权。需要强调的是，当前大多数 NFT 交易平台采用的是全网可见或者平台用户可见，个别平台采用“盲盒”销售模式，仅在购买者支付对价后方能看到其所购买的数字作品。因任何愿意购买的公众依然可以在个人选定的时间和地点进行购买从而获得该作品，故仍然属于信息网络传播权控制范畴。

3. 是否属于著作权法上的“发行”

著作权法上的发行是指权利人通过销售或赠送等转移作品所有权的方式提供作品原件或复制件。随着数字技术的进一步发展，传统权利也扩展到数字领域，以至于对数字作品是否适用于发行权存在不同的认识。尤其针对发行权中的作品原件或复制件是否包含有形和无形产生了诸多分歧。有观点认为，我国著作权法中的发行权定义中的“以出售或者赠与方式向公众提供作品的原

〔10〕 参见前引〔9〕，王迁书，第 164 页。

〔11〕 参见王迁：《复制权与信息网络传播权的关系》，载《湖南师范大学社会科学学报》2022 年第 2 期。

• 73 •

件或复制件”就是指将固定了的作品有形物质载体面向公众进行出售或赠与，即转移物质载体的所有权。〔12〕另一种观点认为，发行权应扩展至网络环境，以出售的方式向公众提供数字作品的复制件，应当落入发行权控制范围。发行权的核心特征在于作品原件或复制件的所有权转让，无关作品载体是有形还是无形。〔13〕我国加入的《世界知识产权组织版权条约》（WIPO Copyright Treat，简称 WCT）明确规定“发行权”是指作者、表演者和录音制作者享有的授权通过销售或其他所有权转让形式向公众提供其作品、录音制品和录制的表演原件或复制件的权利。同时在《通过条约的外交会议的议定声明》中指出，发行权条款中的“复制件”和“原件和复制件”是专指可作为有形物品投放流通的规定的复制件，“原件”是指首次被固定在有形物质载体之上形成的。WCT《基础提案》中亦指出，向公众提供权是指“除了发行复制件之外，使公众能够通过任何的方法和过程获取的权利”。欧盟立法亦采取与 WCT 一样的标准，其在《信息社会版权指令提案》明确发行权的复制件必须固定在有形载体之上，向公众传播权为“除了发行物质复制件之外”的权利。

《著作权法》第 10 条第 1 款第 6 项规定：“发行权，即以出售或者赠与方式向公众提供作品的原件或者复制件的权利。”虽然我国《著作权法》对发行权的载体并未做出明确的规定，但当前理论和实务界主流观点认为应理解为“有形物质载体”，也就是说构成著作权法上的发行行为应当符合以下要件：一是该行为应当面向“公众”提供作品的原件或复制件；二是该行为应当以转移作品有形物质载体所有权的方式提供作品的原件或复制件。笔者同意当前主流观点，理由如下：一是我国作为《世界知识产权组织版权条约》成员国，理应与其保持一致，遵守相应的规定。我国《著作权法》相关内容基本上移植于《世界知识产权组织版权条约》。《著作权法》对“发行权”“信息网络传播权”分别作出了规定，且两者之间的区别是非常清晰的。二是数字作品并没有原件或复制件一说，且数字作品的“发行”表现为“向公众提供作品”而非“向公众提供作品的原件或复制件”，此种情形下的存储作品的物质载体并没有发生转移。三是无论有形载体还是无形载体，发行权一定涉及作品原件或复制件所有权转让，而当前数字作品的“发行”并不产生一种作品原件或复制件所有权的转移。

基于上述分析，笔者认为，在 NFT 交易模式下，虽然 NFT 数字作品交易对象是作为“数字商品”的数字作品本身，交易产生的法律效果亦表现为所谓的“所有权”转移，但因发行权的核心特征在于作品原件或复制件的所有权转让，即当前著作权法中的发行仅限定为有形载体上的作品原件或复制件的所有权转让或赠与，且我国当前法律尚未将“数字商品（虚拟财产）”纳入财产权利范畴予以保护，NFT 数字作品出售并非实质意义上的所有权转让，故 NFT 数字作品出售并不属于发行行为，未经权利人许可将 NFT 数字作品在第三方交易平台的出售行为尚无法落入发行权控制范畴。也即，NFT 数字作品的首次销售以及二次销售等均未侵害著作权人的发行权。需要指出的是，本文将 NFT 数字作品交易排除在发行权控制之外，是基于当前我国《民法典》《著作权法》的相关规定得出的结论。随着数字经济的快速发展，“数字商品”“数字资产”作为交易对象将成为一种常态。中央全面深化改革委员会第二十六次会议强调，要积极推进数据要素

〔12〕 参见前引〔9〕，王迁书，第 175 页。

〔13〕 参见何怀文：《网络环境下的发行权》，载《浙江大学学报（人文社会科学版）》2013 年第 5 期。

市场化，加快构建以数据为关键要素的数字经济，建立数据产权制度，健全数据要素权益保护制度。为此，立法理应及时修改相关法律，对“数字商品”这种虚拟财产的性质给出一个明确的法律身份。一旦“数字商品”纳入财产权利范畴，赋予其所有权法律地位，笔者亦赞同将《著作权法》中的发行权范围进行适当的扩大，将 NFT 数字作品出售纳入发行权控制范畴。

4. 权利穷竭原则在 NFT 数字作品交易中是否适用

权利穷竭原则又称“首次销售原则”或“发行权用尽原则”，〔14〕是指合法获得该作品原件或复印件所有权人可以不经著作权人许可将其再次出售或赠与。权利穷竭原则是著作权法为平衡著作权人与所有权人利益而对发行权进行的限制，目的在于防止著作权人对他人所有权和有形财产的合法流通加以干涉，从而损害合法商品自由流通这一市场经济出现后存在的基本规则。我国《著作权法》虽然并没有明确规定这一原则，且在有形载体发行领域适用权利穷竭原则并无争议。然而，网络环境下数字作品是否适用该原则则产生了三种观点。其中，王迁教授认为，“权利穷竭原则”的价值在于澄清“发行权”与“信网权”之间的界限，数字作品的转售或网络传播属于信息流动，并不发生有形物的转移，发行权用尽当然是失去了存在的基础。也有学者认为，数字作品发行与传统有形作品发行均是以转移作品所有权的方式向公众提供作品，只要以转移所有权的方式向公众提供作品，就应该认定其为发行行为，从而适用“权利穷竭原则”。〔15〕还有观点认为应采用折中路径：权利穷竭原则有条件适用于数字作品发行中，即数字发行权有限用尽。具体而言，根据数字作品的不同类别、不同特性以及不同创作成本等，允许著作权人在一定次数或范围内继续控制数字作品的二次传播，发行权在一定次数或范围内暂时不用尽，超过次数或范围的限制，从而实现著作权人私益与社会公共利益之间的平衡。〔16〕

笔者同意第一种观点。我国著作权法采用了发行权和信息网络传播权分开规定的二元结构。发行权适用于作品的有形载体发生所有权转移的情形，而数字传播行为则全部由信息网络传播权控制，这也是当前司法实践中的通用做法。我国法院表明“复制权和发行权控制的行为需以作品存在于有形载体之上为必要要件，而将作品置于互联网之中系信息网络传播权的保护范围”〔17〕。基于此，笔者认为，NFT 数字作品交易同样亦不能适用权利穷竭原则。其一，如前所述，WCT 第 8 条将数字传输归入向公众传播权，并明确向公众提供权是指“除了发行复制件之外，使公众能够通过任何的方法和过程获取的权利”；WCT《基础提案》中亦指出，初始提供或二次提供均被纳入向公众提供权之中。由此可见，向公众二次提供行为必须经过权利人授权，即上述条约明确将数字作品排除在“权利穷竭原则”之外。而我国作为 WCT 成员国，自然应当与条约规定保持一致。其二，在著作权领域，权利穷竭原则主要适用于发行权权利限制，该原则主要目的是为了防止他人出售作品的非法复制件，而非限制合法售出的作品原件或复制件的使用、处置权利。但著作权领域的“权利穷竭原则”的适用基础是作品与其有形载体的不可分性，是对作品有形载体的使用权利作出规制，具有物理空间和现实操作的可控性。但网络改变了作品的传播方式，公

〔14〕“首次销售原则”是英美法系国家的提法，“权利穷竭原则”“发行权用尽原则”是大陆法系国家的提法。

〔15〕参见前引〔5〕，陶乾文。

〔16〕参见陈全真：《数字作品发行权用尽的解释立场即制度协调》，载《出版发行研究》2021 第 9 期。

〔17〕丁靖文：《论数字作品转售不适用首次销售原则》，载《学术研究》2021 年第 4 期，第 74 页。

众无需转移有形载体就可以获得作品的复制件。这一过程与传统传播途径的根本区别是不会导致作品有形载体在物理意义上的转移。其三，在当前法律框架下，NFT 数字作品虽然可以作为特定化的“数字商品”进行交易，但法律并未赋予其一项财产性权利地位，这意味着 NFT 数字作品交易并非以作品载体所有权的方式提供作品原件或复制件，亦就缺乏了适用“权利穷竭”的前提和基础。同时，在 NFT 交易模式下，不特定公众可以在选定的时间和地点获得 NFT 数字作品，属于典型的信息网络传播行为。这种以信息网络途径传播作品属于信息流动，亦并不导致作品有形载体所有权或占有权的转移，自然不受发行权的控制。当然，本文之所以认为数字作品（含 NFT 数字作品）不适用“权利穷竭原则”，同样是基于当前的立法规定。

三、NFT 交易平台性质及责任边界

根据《信息网络传播权保护条例》及相关司法解释规定，网络服务提供者一般提供自动接入、自动传输、信息存储空间、搜索、链接、文件分享技术等网络服务。由于网络服务提供者不直接向网络用户提供信息或对信息进行组织、筛选和审查，只提供传输通道或者展示平台，相关内容由网络用户提供，故其责任认定时应遵循“避风港规则”和“应知标准（红旗标准）”，适用过错归责原则。然而，随着互联网技术的不断发展，商业模式的不断更新，网络服务提供者逐渐更深度地参与到信息的发布、传播当中，出现了明显不属于上述法律规定情形的“云服务平台”“小程序”“视频分享平台”等一系列新型网络服务提供者。同时，当前大量互联网技术发展，特别是人工智能、算法等技术的普遍使用，二十多年前从美国引进的“避风港规则”所设计的利益平衡和适用环境、技术内容等已经完全不同，亟需构建一套与目前技术状况相匹配的关于网络服务提供者注意义务的机制，以实现动态变化中的利益再平衡。当前，虽然存在不同的意见，但主流观点认为应当给网络服务提供者设置更高的注意义务。对此，笔者认为，对于互联网新技术带来的新类型互联网行为，司法理应秉持谦抑的司法理念，通常情况下不宜轻易做出肯定或否定评价。但是，在当前法律存在空白且亟需明确这些新型网络服务提供者责任边界时，司法应当及时通过个案裁判明确各方主体权利义务，合理界定平台责任，厘清责任边界，规范该新型商业模式市场秩序，发挥司法指引作用，从而引导其依法有序健康发展。对于新型网络服务提供者的责任确定，不能简单地适用现有法律规定予以裁判，而是应当根据网络服务提供者的具体服务方式、经营模式、控制能力、技术特点等因素，综合运用比例原则、利益平衡原则和权利义务一致原则等予以综合认定。

根据经营方式不同，NFT 平台主要分为自营和他营两种模式；根据入驻方式不同，NFT 平台主要分为邀请制和注册制；而根据是否允许二次交易可分为 NFT 交易平台和 NFT 非交易平台。本文仅针对采取他营模式和注册制的 NFT 交易平台进行探讨。从 NFT 交易平台提供的交易模式和服务内容来看，其系专门提供 NFT 交易服务平台，交易的 NFT 数字作品由平台注册用户提供，且不存在与用户以分工合作等方式参与 NFT 数字作品交易，故此，根据当前法律的相关规定，NFT 交易平台应属于网络服务提供者而非内容提供平台。NFT 交易平台作为一种为注册用户提供 NFT 数字商品交易服务的平台，明显不属于“提供自动接入、自动传输、信息存储空

间、搜索、链接、文件分享技术等网络服务”中的任何一种网络服务平台。NFT 数字作品交易系伴随着互联网技术发展，并结合区块链、智能合约技术衍生出现的网络空间“数字商品”交易模式创新，属于新型商业模式。有学者称其“在国内外的数字版权交易活动中，在有效解决确权难、实现去中心化交易方面发挥了显著作用”〔18〕。对于像本 NFT 案所涉 Bigverse 平台这种提供 NFT 数字作品交易服务的网络平台的责任边界，应结合 NFT 数字作品的特殊性及 NFT 数字作品交易模式、技术特点、平台控制能力、经营模式等方面综合认定。〔19〕

首先，从 NFT 数字作品交易模式来看，NFT 数字作品作为交易客体时表现为特定的“数字商品”，既涉及作为数字作品的著作权，也涉及作为“数字商品”的“所有权”。如前所述，NFT 交易模式下产生的法律后果将包括“所有权”的转移。因此，NFT 数字作品的铸造者（出售者）应当是作品原件或复制件的所有者。同时，根据《著作权法》的相关规定，所有权发生转移，但作品著作权并未发生改变。在 NFT 交易模式下，NFT 数字作品的铸造者（出售者）将 NFT 数字作品复制、上传至平台进行交易的行为，分别为《著作权法》中的复制权、信息网络传播权所控制，因此，NFT 数字作品的铸造者（出售者）不仅应当是作品复制件的所有者，而且应当系该数字作品的著作权人或授权人，否则该 NFT 数字作品属于明显侵害他人著作权的侵权商品。对此，Bigverse 平台作为专门从事 NFT 数字作品交易服务平台知道也应当知道，且理应采取合理措施防止侵权发生，审查 NFT 数字作品来源的合法性和真实性，以及确认 NFT 铸造者获得适当权利或许可来从事这一行为。换言之，Bigverse 平台对用户上传用于铸造 NFT 的数字作品相关权利应当进行合理的事先审查，以防止该 NFT 数字作品存在权利瑕疵，侵害他人著作权。

其次，从 NFT 数字作品交易采用的技术来看，整个交易模式采用的是区块链和智能合约技术。作为区块链技术下的一个新兴应用场景，NFT 不仅解决了数字作品作为商品时的可流通性和稀缺性（非同质化），而且能够解决交易主体之间的信任缺乏和安全顾虑，构建了一种全新的互联网新业态之诚信体系。其中，NFT 数字作品之所以具有投资价值和收藏价值，最核心原因之一是基于区块链中的信任机制，智能合约是承载交易双方合意的载体，Bigverse 平台上的每一次交易因智能合约中已嵌入了“自动执行”代码将自动触发完成。因此，如果 NFT 数字作品存在权利瑕疵，不仅将破坏交易主体以及 NFT 交易平台业已建立的信任机制，而且将严重损害整个交易秩序的确定性，进而损害交易相对人的合法权益以及著作权人的权益。同时，因整个交易系通过智能合约由代码自动执行，交易次数将无法人为控制，且 NFT 数字作品交易属于信息网络传播行为，并不适用权利用尽原则。因此，一旦 NFT 数字作品构成侵权，往往会损害数个甚至几十个善意交易相对方的合法利益，导致交易双方纠纷频发，动摇 NFT 商业模式下的信任生态，将严重妨碍整个 NFT 行业的有序发展。

再次，从 Bigverse 平台控制能力来看，一是，所有 NFT 交易形成的数据均保存于 Bigverse 平台网络服务器中，特别是用户上传作品后至完成 NFT“铸造”前，均是由 Bigverse 平台控制整个流程以及所有内容，因此，Bigverse 平台具有较强的控制能力。二是，从 Bigverse 平台 NFT 数字作品铸造流程来看，用户按照平台要求，完成上传作品并提交后即进入平台审核环节，

〔18〕 薛晗：《基于区块链技术的数字版权交易机制完善路径》，载《出版发行研究》2020 年第 6 期，第 51 页。

〔19〕 参见杭州互联网法院（2022）浙 0192 民初 1008 号民事判决书。

· 77 ·

只有审核通过的才能上架，最终作为 NFT 数字作品在 Bigverse 平台上进行交易。可见，对 NFT 数字作品进行一定形式上的审查原本就是 Bigverse 平台所设置的必备流程之一。因此，赋予 Bigverse 平台一定的审查义务，并没有直接增加平台义务。三是，从 Bigverse 平台审查的对象来看，每个用户每次提交审查的均为单个作品，并不存在海量的数据内容，不会出现平台无法一一审查的情形。故此，Bigverse 平台对其平台上交易的 NFT 数字作品不仅具有较强的控制能力，而且也具备相应的审核能力和条件，同时亦并没有额外增加其审查内容和控制成本。

最后，从 Bigverse 平台的经营模式来看，其不同于电子商务平台和提供存储、链接服务等网络服务平台，并非免费或者采取会员费等方式获取经济利益，而是系直接通过佣金等方式从 NFT 数字作品交易中获得利益。从 NFT 数字作品交易流程来看，Bigverse 平台不但在铸造时收取作品燃费，而且在每次作品交易成功后收取一定比例的佣金及燃费。笔者认为，平台获得的经济利益应与其注意义务相适用，在平台用户的权利与著作权保护之间保持一种平衡。既要从兼顾行业利益格局、主体利益分配和成本效率权衡三个维度进行考量，以实现各方主体的利益平衡，又应充分发挥司法引导作用，避免各方利益失衡的情况发生。《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》第 11 条第 1 款规定：“网络服务提供者从网络用户提供的作品、表演、录音录像制品中直接获得经济利益的，人民法院应当认定其对该网络用户侵害信息网络传播权的行为负有较高的注意义务。”Bigverse 平台这种营利模式明显属于上述法律规定范畴，即在 NFT 数字作品中直接获得经济利益，其自然应承担较高的注意义务。

综上，笔者认为，NFT 交易平台不仅需要履行一般网络服务提供者的责任，还应当承担较高的注意义务，包括但不限于对 NFT 数字作品权利的事先审查、明知或应知侵权时的主动下架删除等义务，否则应承担相应的法律责任。NFT 案中，Bigverse 平台正因为其未履行相应的审查义务，最终被法院认定构成帮助侵权。NFT 交易平台在履行上述注意义务时，理应建立一套有效的知识产权审查机制，对平台上交易的 NFT 作品的著作权做初步审查，如审查申请 NFT 铸造的用户是否提供了涉及著作权底稿、原件、合法出版物、著作权登记证书、认证机构出具的证明等初步证据证明其为著作权、与著作权有关权益的权利人。当然，这种审查应当是基于网络服务提供者具有的善良管理者义务角度进行评价，并且应赋予网络服务提供者一定的自主决策权和审查空间，可以在法律规定的框架内，根据自身审查需要、知识产权权利类型、产业发展等实际情况等因素，对具体要求进行明确和细化。从判断标准来看，应当采用“一般可能性”标准。也就是说，该初步证据应当排除明显不能证明是著作权、与著作权有关权益权利人的证据，并具有使得一般理性人相信存在权利的可能性即可。同时，NFT 交易平台还应构建相应的侵权预防机制，形成有效的筛查、甄别体系，从源头上防止侵权发生，必要时可要求铸造用户提供担保机制，最大限度防止 NFT 数字作品存在瑕疵，以防止侵权发生。

四、侵权责任承担方式的探索

按照侵权责任法的相关原理，“停止侵害”是侵权责任中最主要也是最重要的责任承担形式。我国《著作权法》亦秉持侵权责任法一般规定精神，明确著作权侵权人应当承担停止侵权责任。

也就是说，在 NFT 案中，Bigverse 理应立即删除侵权 NFT 数字作品等侵权内容，停止侵权。然而，根据 Bigverse 平台服务协议，Bigverse 平台对侵权的“NFT 数字作品”可以采取的措施仅为删除、屏蔽、断开侵权链接，无法将该“数字作品”对应的非同质化通证（NFT）及其他上链侵权内容予以删除。因 NFT 系采用区块链技术进行同步保存数据的，NFT 数字作品及其交易的相关数据均保存于区块链服务器和各节点服务器中。区块链中各节点均为匿名，且“共识机制”是区块链中各节点之间必须遵守的处理机制。故此，通常而言，各区块链节点之间无法形成共识，进而无法删除以哈希值形式存在的侵权数字作品所对应的“NFT”以及交易的相关数据。因该“NFT”及其交易的相关数据仍然保留在 NFT 交易平台服务器中，侵权内容并没有删除，理论上仍存在侵权的可能性，显然并没有达到“停止侵害”之法律效果。因此，NFT 案中最终采用 Bigverse 平台将该侵权 NFT 数字作品在区块链上予以断开并打入地址黑洞之方式以达到停止侵权的法律效果。笔者认为，NFT 案中对停止侵权的责任承担方式的处理无疑是一种契合区块链等互联网技术而创新的探索，一方面可以实现停止侵权的效果，另一方面又兼顾了 NFT 交易模式的技术特点，妥善平衡了 NFT 数字作品侵权中各方主体的利益，较好地解决了 NFT 交易模式下“停止侵权”这一棘手的问题，亦为今后类似案件的处理提供了新的思路和参考。

同时，笔者认为，除了 NFT 案所探索的责任承担方式之外，也可以探索“著作权侵权不停止制度”在 NFT 侵权责任承担中的适用。在知识产权领域，“侵权不停止”最早出现在美国司法判例中，其实质属于对权利人行使权利的一种限制，系关于知识产权保护的例外规定和利益平衡的有效手段。这种平衡机制不仅对知识产权人专有权给予保护，而且应当保护其他私权利、公共利益以及公平竞争等。〔20〕 也就是说，通过适当限定知识产权人的专有权利，调整知识产权人与公众、利益关系人的关系，合理兼顾各方利益，使之处于利益平衡状态，以彰显立法的灵活性和司法的能动性和智慧性。〔21〕 侵权不停止制度主要适用于对私人与公共利益、私人与私人利益平衡之情形。“侵权不停止”制度在我国最早出现在司法政策中。2009 年《最高人民法院关于当前经济形势下知识产权审判服务大局若干问题的意见》第 15 条指出，如果停止有关行为会造成当事人之间的重大利益失衡，或者有悖社会公共利益，或者实际上无法执行，可以根据案件具体情况进行利益衡量，不判决停止行为，而采取更充分的赔偿或经济补偿等替代性措施了断纠纷。之后，2016 年颁布的《最高人民法院关于审理侵犯专利权纠纷案件应用法律若干问题的解释（二）》第 26 条规定：“被告构成对专利权的侵犯，权利人请求判令其停止侵权行为的，人民法院应予支持，但基于国家利益、公共利益的考量，人民法院可以不判令被告停止被诉行为，而判令其支付相应的合理费用。”这是我国知识产权立法首次对这一制度作出规定。虽然我国《著作权法》及相关司法解释并没有明确规定侵权不停止制度，但其现已成为立法和司法的新趋势，尤其是被不断适用在著作权侵权案件中。比如“大头儿子”著作权纠纷案、〔22〕 中国音乐著作权协会与长安影视公司等著作权侵权纠纷案、〔23〕 正东公司与东上海分公司等著作权侵权纠纷案〔24〕等。可见，“著

〔20〕 参见田小军、刘洋：《“侵权不停止”在知识产权案件中的适用问题》，载《中国版权》2016 年第 6 期。

〔21〕 参见徐清云、张波：《著作权侵权不停止的利益平衡理论》，载《四川职业技术学院学报》2018 年第 4 期。

〔22〕 参见杭州市中级人民法院（2015）浙杭知终字第 356 号民事判决书。

〔23〕 参见北京市第一中级人民法院（2003）一中民初字第 2336 号民事判决书。

〔24〕 参见北京市朝阳区人民法院（2012）朝民初字第 12869 号民事判决书。

· 79 ·

作权侵权不停止”可以适用于著作权侵权纠纷中已经成为一种共识。正如有学者所言，《著作权法》第 53 条中的“应当根据情况”可理解为法律不要求停止侵害责任一律适用，即法院可以根据个案的具体情况自由裁量做出判决，通过以赔偿方式替代侵权责任的司法指导意见同样适用。〔25〕

笔者认为，作品的价值在于传播，著作权本身具有一定的社会公共属性。从这一角度上讲，“著作权侵权不停止制度”既符合我国著作权法所提倡的促进科学和文化事业发展与繁荣的根本目的，亦符合著作权法的基本原理。在 NFT 数字作品著作权侵权纠纷中，一方面因 NFT 采用了区块链技术来保障交易，实际上无法真正完全执行“停止侵权”之责任承担；另一方面，NFT 交易是通过智能合约执行的，整个交易次数无法人为控制，因此一旦停止侵权往往会涉及多个善意交易主体的合法利益，既不利于整个 NFT 商业模式的发展，也会动摇 NFT 交易中的整个信任机制。同时，NFT 交易模式下的著作权侵权大多数针对侵害著作财产权，这也为用经济补偿（类似于支付许可使用费）替代停止侵权提供了可能。因此，在 NFT 数字作品著作权侵权纠纷处理中，为了调整著作权人、NFT 数字作品交易相对人与社会公众的利益关系，使之处于利益相对平衡状态，可用更充分的赔偿或经济补偿来替代“停止侵权”之责任承担，在充分保障著作权人合法权益的基础上，实现 NFT 交易主体之间的利益平衡，从而推动 NFT 交易这种新型商业模式有序健康发展。

Abstract: In recent years, NFT transaction, as a new business model, has developed rapidly, and it also brings challenges to the current legal order and produces a series of new problems. It is also urgent to regulate the NFT market, clarify the boundary of responsibility of relevant subjects, protect the legitimate rights and interests of all parties according to law, so as to guide the healthy and orderly development of the NFT market. It is necessary to analyze and study new legal issues such as the nature of behavior under the NFT mode, the boundary of liability of NFT trading platform, whether the exhaustion of rights principle applies to digital works, and the way of bearing tort liability, based from the copyright issues reflected in judicial cases. NFT digital works trading is not the distribution of copyright law, and should be included in the control of information network transmission rights. NFT trading platform is a new type of network service provider. Considering the legal attributes of NFT trading mode, technical characteristics, platform control ability, profit mode and other factors, it should assume a high duty of care. The mode of NFT tort liability shall be reasonably determined based on the characteristics of blockchain technology.

Key Words: NFT, information network dissemination, platform responsibility, infringement does not stop

（责任编辑：张金平　赵建蕊）

〔25〕 参见前引〔21〕，徐清云、张波文。

财经法学 No. 6，2022
pp. 125 - 136

元宇宙的法律难题

［印尼］萨法里·卡西亚安托　［德］穆斯塔法·基林茨　著
郑志峰　罗有成　译*

内容提要：在社交媒体巨头的首席执行官宣称元宇宙将成为继互联网之后的下一个大事件后，元宇宙获得了良好的发展势头。虽然目前还没有统一、共识性的元宇宙定义，但对元宇宙的共同理解是该概念结合了 IoT、AR、VR、XR 和 3D 技术。元宇宙蕴含巨大的市场资本和经济潜力，因此，讨论元宇宙的法律含义至关重要。本文是第一篇以恰当的方式阐述元宇宙的法律难题的文章。它包括对一般物权法和知识产权法的讨论，以及是否已经到了需要制定“虚拟财产法”的时候。它还讨论了隐私和数据保护、合同法、网络安全和网络攻击、货币和支付系统法、虚拟资产法规、税法、反洗钱法和了解客户规则，以及刑法等其他法律问题。元宇宙创造了一个现实世界法律可能难以适用的新空间。因此，元宇宙破坏了法律权威的“传统主张”、扰乱了尊重法治的需求。然而，将现实世界的法律适用于元宇宙仍然是可能的，但有局限性。当在元宇宙实施现实世界的法律时，这种局限性就会具体地表现出来。

关键词：元宇宙　法律难题　虚拟世界　货币法　支付系统法

一、引　言

自从 2019 年新冠肺炎疫情暴发后，全球经济的增长势头开始放缓。在新冠肺炎疫情暴发之

* 萨法里·卡西亚安托，蒂尔堡大学经济与法律研究中心研究员；穆斯塔法·基林茨，德国奥托贝森商学院助理研究员；郑志峰，西南政法大学民商法学院副教授、网络空间治理研究院副院长；罗有成，西南政法大学网络空间治理研究院助理研究员、博士研究生。

本文为 2020 年国家社科基金青年项目“人工智能与《民法典》双重背景下个人信息保护研究”（20CFX041）、2020 年国家社科基金重大项目“数字社会的法律治理体系与立法变革研究”（20&ZD177）的阶段性成果。

原文发表于《中央银行法律与制度杂志》（Journal of Central Banking Law and Institutions），感谢作者和期刊的慷慨授权。经作者同意，译者在此省略了引文。

前，全球经济增长达到了 2.8%，其中，发展中国家增长了 3.7%，发达经济体仅增长 1.7%。在新冠肺炎疫情暴发期间，全球经济增长大幅收缩，在 2020 年下降了 3.1%，伴随着大多数经济行业的人均产出的普遍下降。这是自 19 世纪 70 年代长期经济大萧条以来的最大降幅。尽管预计 2021 年全球经济增长将会触底反弹至 5.7%，但这场疫情对于经济的损害已经造成，并且留下了不可磨灭的创伤。新冠肺炎疫情造成人员流动严重受阻、城市封锁、各个经济体国边界关闭，人们进入防疫或者隔离状态。大多数经济行业的市场规模急剧下降。〔1〕以受疫情影响最严重的行业之一——旅游业——为例，2020 年市值同比下降了 70%，几乎是一夜之间回到了 30 年前。由此可见，世界的经济正面临着前所未有的危机。

然而，在新冠肺炎疫情重创经济并引发各种社会危机的同时，数字化（digitalisation）却迎来了蓬勃发展。伴随着所谓的“新常态”，使用数字技术和创新已经成为公众的一种新的生活方式。居家远程办公变得无处不在，〔2〕虚拟会议非常普遍，〔3〕在线和远程学习增加，数字交易也创下了历史最高记录。为了克服旅游业的下滑，政府和企业开始使用虚拟现实（VR）等数字活动来吸引游客。在印度尼西亚，2022 年第一季度使用电子货币的交易额同比增长了 42.06%，而使用数字银行平台的交易额同比增长了 34.9%。预计到 2022 年，整体电子交易将同比增长 18.03%，电子货币将达到 360 万亿卢比，数字银行将同比增长 26.72%，达到 51729 万亿卢比。

在新冠肺炎疫情后，数字化的势头继续增强。2021 年 10 月，社交媒体巨头 Facebook 的首席执行官马克·扎克伯格（Mark Zuckerberg）宣布，元宇宙是下一个大事件（the next big thing），是互联网从当前 Web 2.0 迈向未来 Web 3.0 的一场革命。扎克伯格甚至将公司的名称更改为 Meta，并承诺将投入 100 亿美元用于元宇宙的开发。在这个新的虚拟世界——元宇宙——中，人们可以像在现实世界中一样，使用化身（avatars）来行动、互动以及进行商业活动。2021 年 12 月，有人支付了 45 万美元购买虚拟土地。〔4〕无独有偶，Token.com 的首席执行官安德鲁·克里格尔（Andrew Kriggel）花了 240 万美元的高价在元宇宙时尚区买了一块虚拟土地，〔5〕与公众人物史努比·道格（Snoop Dogg）做起了邻居。元宇宙创造的世界可能是虚拟的，但围绕它们的经济交易却是真实的，对现实世界的影响也是实实在在的。因此，元宇宙中的交互可以在关联的各方主体之间产生权利和义务。这种权利和义务可以是基于社会、伦理或者法律规范而产生的，就像现实世界那样，因为虚拟世界的居民实际上是现实世界中真实的人。随着虚拟（线上）世界和现实（线下）世界的碰撞，法律规则在元宇宙场景下的适用就出现了一系列难题。这些难题主

〔1〕以印度尼西亚为例，其大部分经济行业在 2020 年大幅下滑，其中，最严重的行业是交通和物流行业（下降了 15.04%）以及住宿服务和食品饮料行业（下降了 10.22%）。只有少数行业，如卫生和社会服务行业、信息通信技术（ICT）行业保持着高效的增长率，分别为 11.6%和 10.58%。总体而言，印度尼西亚的经济在 2020 年下降了 2.07%。

〔2〕元宇宙中的远程办公可以促使人们远离大城市。也许，元宇宙可以成为政府更好地将居民安置在城市和郊区之间的工具。

〔3〕据研究统计，在线平台 Zoom 的日常会议参与者从 2019 年 12 月的 1000 万人激增至 2020 年 3 月的 2 亿人。尽管 Zoom 平台存在安全问题和网络攻击，但在线平台会议的使用量增加了 2000%，其原因就是新冠肺炎疫情的暴发。

〔4〕在涉及虚拟房地产这一商业活动时，Sandbox（沙盒）被认为是最大的元宇宙平台，其拥有大约 62%的可用元宇宙土地。2012 年，Sandbox 还是一款在线视频游戏。2021 年 11 月，Sandbox 已经转变为元宇宙。

〔5〕这个元宇宙平台名为 Decentraland。2015 年，Decentraland 作为开源 3D 世界建立。与沙盒不同的是，Decentraland 的土地是有限的，其元宇宙土地只能由社区成员获得。

要包括现实世界中的法律如何在元宇宙中适用、谁将颁布元宇宙独有的法律、谁将在元宇宙中执法，以及谁将保护元宇宙社会并维持其秩序。

本文详细阐述了元宇宙引发的一系列法律难题。为了更好地进行分析，本文考察了技术进步是如何冲击法律权威，又是如何违背法治要求的。罗杰·布朗斯沃德（Roger Brownsword）指出，技术对于法律的冲击可以分为三种：第一种技术冲击挑战了国家法律权威机构的主张，即作出决策的权力、决策或者法令获得遵守的法律约束力。当智能技术创造出传统法律难以适用的新空间时，这种情况就会发生。例如，网络空间的互动涉及多个司法管辖区、多个国家的公民、复杂而新颖的行为，以及使用虚拟货币或财产的跨境支付。第二种技术冲击破坏了法律原理，即法律应该受到尊重仅仅因为它是法律。当人类的行为不再需要由人类来统治，而是全面受制于技术时，这种情况就会出现。第三种技术冲击对于法律的破坏更为深远。因为它侵蚀的是我们对于权威和尊重法律的概念性思维。当智能技术支配了所有人类行为（当然是在某些领域）的时候，我们所熟悉的关于法律权威的传统思维以及尊重法律的要求，都会变得过时。

本文认为，元宇宙对法律产生的冲击属于第一种。元宇宙破坏了法律权威的“传统主张”和尊重法律的要求。因此，元宇宙的法律和治理就成为一个亟待解决的难题。本文试图通过将元宇宙中的法律、治理和伦理问题作为在现实世界中发生的问题来讨论，进而尝试解决这些问题。尽管这种方法并不完美，但作为解决这一难题的首次尝试，它还是有用的。

本文是第一篇以恰当的方式系统阐述元宇宙的法律难题的文章。此前关于元宇宙的研究主要包括元宇宙的开发方法、元宇宙的技术方面、元宇宙的治理和伦理方面，以及元宇宙法律方面的一些具体问题，尤其是隐私和数据保护。本文的独特价值在于，对元宇宙的法律问题进行了较为全面的分析，包括物权法、知识产权法、合同法和智能合约、货币和支付系统法、加密资产法规、税法、反洗钱法和了解客户（know your customer）规则，以及刑法。根据我们的了解，现有的研究都还没有讨论元宇宙中有关货币和支付系统法或税法的问题。

本文结构安排如下：第二部分概述了元宇宙的理论和实践，作为我们认识元宇宙中行为的基础；第三部分讨论了元宇宙中行为引发的法律和伦理问题，首先包括物权法和知识产权法（以及当下是否需要制定“虚拟财产法”）、隐私和数据保护、合同法和智能合约、货币和支付系统法，另外，本文讨论的其他法律问题还包括诸如证券和大宗商品法等虚拟资产法规、税法、反洗钱法和了解客户规则、刑法；第四部分提供了一个结论。

二、元宇宙：理论与实践

在这一部分中，我们将讨论元宇宙的理论及其实践。在这些元宇宙实践中，出现了独特的法律和伦理问题。在理论维度，我们将概述元宇宙的概念、经济和技术性细节，以及元宇宙中使用的货币和支付系统。在实践维度，我们将解释元宇宙的应用，因为它们是元宇宙用户之间法律关系的来源。这两个维度的讨论，将作为元宇宙法律分析的基础。

（一）元宇宙的概念

目前没有一个统一、共识性的元宇宙概念。“元宇宙”一词最早由尼尔·斯蒂芬森（Noel

Stephenson）在 1992 年的科幻小说《雪崩》（Snow Crash）中提出。在《雪崩》中，斯蒂芬森用“元宇宙”来描述一个乌托邦，以避免现实生活中的反乌托邦。如今，“元宇宙”这一概念已经扩展到包括虚拟世界中的真实活动。这样的虚拟世界通常配备了增强现实（AR）、虚拟现实（VR）、扩展现实（XR）、3D 技术以及物联网（IoT）技术。元宇宙也被称为 Web3.0，是当前 Web2.0 状态的下一代互联网。

从词源上讲，“元宇宙”一词来源于 meta 和 universe 这两个词。meta 的意思是“之后”“在……之后”“转变”或“超越”。帕克和金（Park & Kim）的一项研究很好地提炼了元宇宙的许多定义。在该项研究中，他们提供了从 54 项研究汇总而来的元宇宙的广泛定义。然而，元宇宙最常见的概念，是指用户使用化身来行动/交互的虚拟世界，以及作为一种媒介、通过用户的化身去连接用户的扩展现实技术（XR）。元宇宙的最新概念与其早期版本（例如游戏《第二人生》的版本）的不同之处在于，它是第一个使用 Z 世代的社会价值观开发的，Z 世代认为线下世界和线上世界根本没有什么区别。

（二）元宇宙的经济

2021 年 10 月，元宇宙公司总市值为 14.8 万亿美元。其中，包括市值 155 亿美元的 Roblox、市值 19.3 亿美元的 Sandbox 和市值 19 亿美元的 Decentraland。图 1 展示了元宇宙的市场参与者。

图 1　元宇宙的市场图（6.1 版本，2021 年 11 月 24 日更新）

值得注意的是，虽然目前的元宇宙状态尚未发挥其全部的潜力，但它已经展示了巨大的经济潜力。早期的研究表明，元宇宙的市场潜力在 3.75 万亿美元到 12.46 万亿美元之间。这或多或少受到了元宇宙狂热者的最近推动，特别是加密货币和非同质通证（non-fungible tokens，又译“非同质代币”，简写为 NFTs）用户的推动。如图 2 所示，2022 年 5 月，通过元宇宙应用程序进行的销售的全球日销售额飙升到了 6 亿美元。

元宇宙的经济问题包括初创企业和现有企业之间的竞争问题，以及运营元宇宙对社会福利的

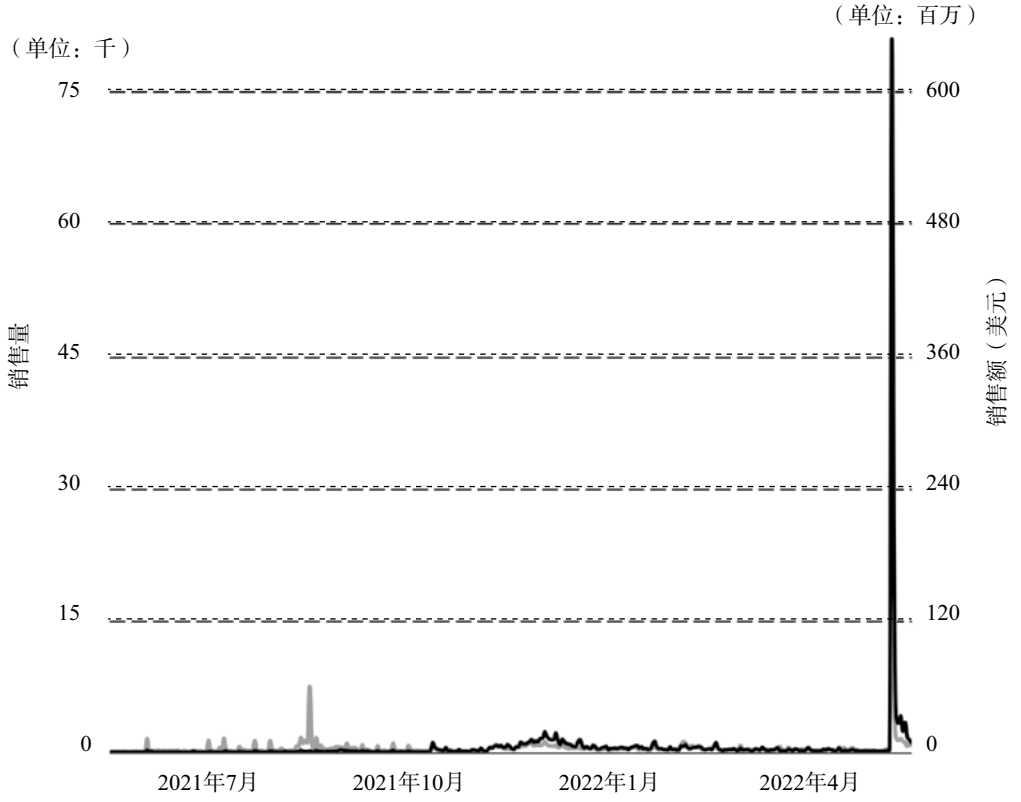

图 2 过去一年通过元宇宙应用程序的每日销售额〔6〕

影响。元宇宙是凯恩斯主义的需求驱动型创新，因此内嵌在元宇宙中的“按需”（on-demand）产品/服务将成为其优势。正如我们所知，这可能会导致元宇宙对传统商业的破坏，或者元宇宙仍然停留在一个乌托邦的设想上。

（三）元宇宙的分类

由于元宇宙目前仍处于早期阶段，许多研究都提出了不同的分类方法，以便我们更好地理解元宇宙这个概念。其中，一项突出的研究是帕克和金提供的元宇宙分类。他们提出了实现元宇宙概念的三大构成和三种方法：三大构成是物理设备和传感器（硬件）、识别和渲染（软件）以及场景生成（内容）；而三种方法则包括用户交互、实施的技术方法和元宇宙应用。图 3 显示了用于实现元宇宙概念的每个构成部分和方法的详细信息。

在这项研究中，值得注意的是元宇宙应用程序的关键作用，因为它们将作为法律权利和义务的基础。这些应用程序包括模拟、游戏、办公、社交、营销、教育和经济交易。

（四）元宇宙使用的货币和支付系统

元宇宙中的活动都通过加密货币、非同质通证或代币等支付手段而绑定起来。这些虚拟资产充当了元宇宙联通现实世界的经济桥梁。有人可能会说，这些虚拟资产确实赋予了元宇宙更深的

〔6〕 数据来自 https：//nonfungible. com/market-tracker.

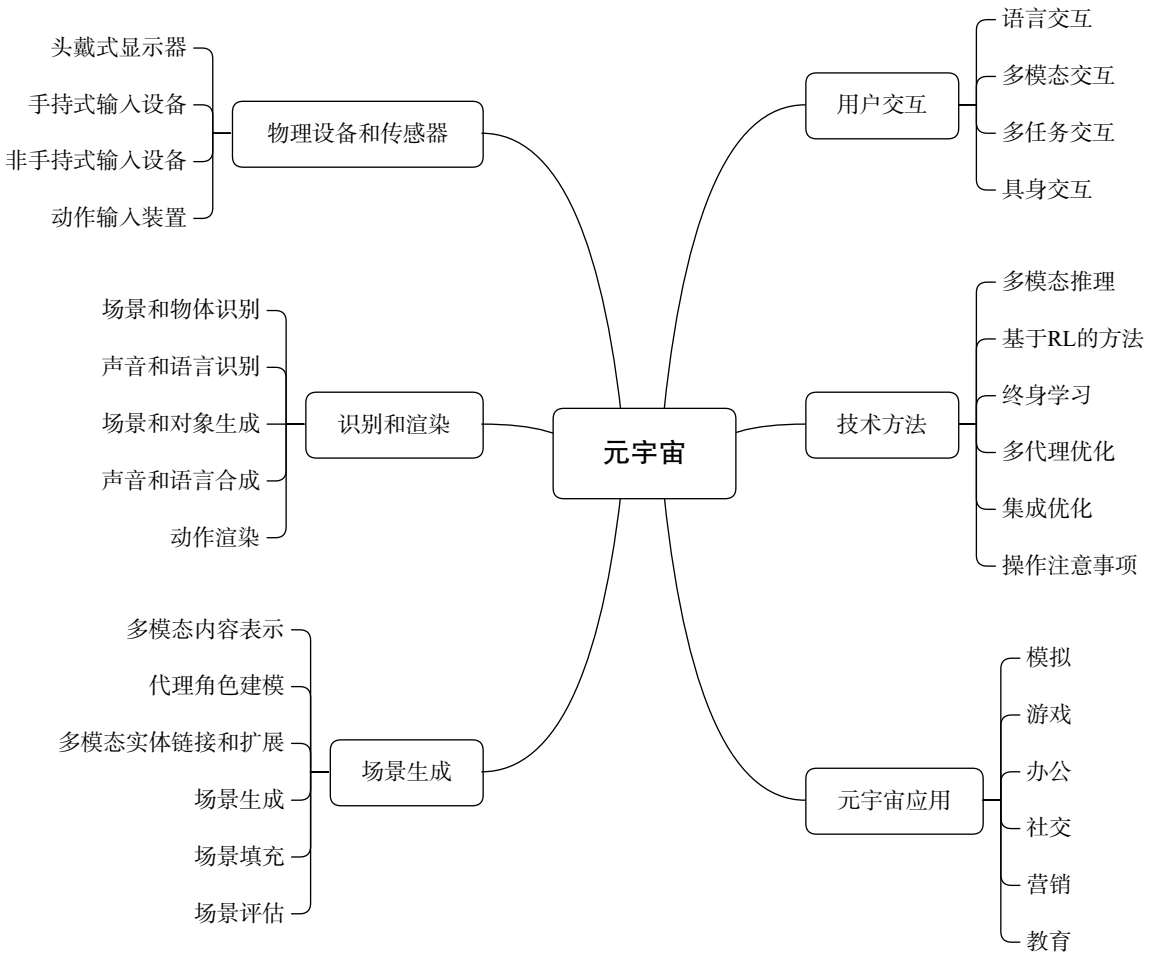

图 3　帕克和金的元宇宙分类

社会和经济意义。例如，Decentraland 使用 Polygon Mana 这种加密货币，而 Sandbox 使用的加密货币是 Sand Crypto。在加入元宇宙之前，用户必须为自己创设数字钱包，用户可以在数字钱包中存放如 Mana 和 Sand 之类的加密货币、非同质通证或代币。

三、元宇宙的法律难题

本部分主要围绕元宇宙有关的法律问题展开讨论，涉及元宇宙的各种应用和各方主体。根据上述元宇宙的理论和实践，我们归纳了元宇宙中的七种行为类型，包括模拟、游戏、办公、社交、营销、教育和经济交易。当然，所有这些行为都是以虚拟形式进行的。从这些类型化的行为出发，我们分析了相关的法律问题，并在以下各小节中进行讨论。

（一）物权法和知识产权法：需要一部“虚拟财产法”吗？

第一个也是最关键的法律问题，即物权法和/或知识产权法是否可以在元宇宙中适用。或者说，一个明显的问题是，制定一部“虚拟财产法”的时机是否成熟。

通常来说，物权法调整使用物并排除他人使用该物的权利。它回答了两个常见的难题：（1）谁

有权使用该物；（2）他们如何获得这项权利。物权法的常见例子是土地或个人物品（例如自行车或椅子）的使用。物权法的目标是为各种利益、使用权之间的分配提供一种公正、可预测、透明的手段。

在元宇宙中，所有的物都是虚拟的，且使用和存储方式同样是虚拟化的。它们不同于物权法中的有体物，有体物在物理上可以位于特定位置。虽然物权法制度可以用于解决无体物的使用问题，但不能解决权利使用的分配问题。因此，物权法基本无法适用于元宇宙。

知识产权法可能在本质上更适用于元宇宙。与传统的物权法不同，知识产权法调整的客体不一定是可以在物理上放置的有体物。知识产权法调整无体物的权属、享有的权利以及其衍生的权利形式。这些权利包括专利权、版权和商标权。

研究知识产权如何在元宇宙中发挥作用至关重要。按照一种非常传统的方式，元宇宙中的权属可以分为两种不同的类型。第一种是虚拟世界中一切财产的权利属于平台提供商（platform provider）。在这种情况下，用户只能从平台提供商处获得使用此类物的许可。游戏《魔兽世界》（World of Warcraft）〔7〕就是一个例子。根据《魔兽世界》的《服务条款》，平台内的所有权利、资格和利益均属于平台提供商。这包括用户账户、数据、计算机代码、虚拟商品（如货币和数字卡）、所有角色，甚至角色的名字。〔8〕第二种是允许用户拥有某些财产。游戏《第二人生》就是一个很好的例子。根据《第二人生》的《服务条款》，用户将保留任何法律上承认的权利，包括版权等知识产权。〔9〕

然而，第一种权利模式无法适用于元宇宙。对于元宇宙来说，只有第二种权利模式是可能的，其中用户有权拥有某些财产。这是因为，在元宇宙中，用户的行为模仿了现实世界，包括拥有土地和/或房屋（当然是虚拟的）的权利、拥有进行交易的货币（当然还有加密货币），或者创造、购买和出售非同质通证或代币。〔10〕如果在元宇宙中适用第一种权利模式，元宇宙就无法发挥其最大潜力。也许，这样的平台根本就不能被称为元宇宙。

如果允许元宇宙中的任何用户拥有某些财产，那么下一个问题将是，现有的知识产权法是否足以保护用户知识产权免受他人的侵犯。与规制有体物的物权法不同，知识产权法乍一看似乎是完美的。但是，知识产权法在法律实施方面会显现出局限性。由于元宇宙的行为跨越了不同司法管辖区并涉及不同国家的主体，法律管辖权、法律选择和执法权等问题就导致现有知识产权法在元宇宙中的适用具有不确定性。

（二）隐私和数据保护

当我们从公开透明原则来考虑元宇宙时，隐私问题就会出现。然而，人们加入元宇宙的动机

〔7〕《魔兽世界》是暴雪娱乐在2004年发行的一款最受欢迎的大型多人在线角色扮演游戏。根据Statista数据平台统计，《魔兽世界》现在拥有大约475万活跃用户。

〔8〕参见暴雪最终用户许可协议的第2条。

〔9〕例如，《服务条款》第1.2条第1款规定的“……你（用户）保留你在你的用户内容中拥有的任何法律上承认的权利、资格和利益”，以及第2.3条第1款规定的“你在你上传、发布和提交的内容中保留你法律上拥有的任何和所有知识产权……”。

〔10〕与此同时，有学者针对这一问题也提供了类似的分析，但使用了不同的术语。例如，有学者［迈克尔·周（Zhou）、马克·林德斯（Leenders）、凌美聪（Cong）］指出，元宇宙中有两种不同的权利框架，即平台所有权和内容所有权。这两个所有权框架对元宇宙来说至关重要。

始终是享受社交互动，包括与他人共享个人数据与信息。由于元宇宙是为开放和透明而设计的，因此信息共享是无条件的。在现实世界中，人们在与他人互动时完全掌控着自己的个人信息。然而，这显然不符合元宇宙的实际情况。因此，监管机构需要对元宇宙平台提供商进行监管，以优先考虑元宇宙用户的隐私。

第二个隐私问题涉及侵犯隐私权。就像在现实世界中一样，人们在元宇宙中同样爱管闲事和充满好奇。在元宇宙中的社交互动中，用户与用户之间往往有更多的接触，因为元宇宙中的“生活”对他们来说更加奇幻。这种动机和行为可能会使隐私处于危险之中。一旦发生隐私泄露，元宇宙平台提供商只有非常有限的机制来降低隐私泄露的负面影响。

另一个问题与用户的数据保护有关。元宇宙存储和管理着用户的大量数据，包括个人数据。元宇宙的数据流量非常巨大，从而导致了一些数据控制问题。这还没有考虑与跨境数据流动相关的问题，因为元宇宙的用户通常来自数百个国家。[11] 下面这些棘手的问题已经显现出来：（1）元宇宙平台提供商在多大程度上有义务遵守隐私和数据保护法，例如遵守严格的欧盟数据保护方面的法律法规；（2）数据保护机构是否有权对其管辖范围以外的元宇宙平台提供商执法。

（三）合同法和智能合约

元宇宙中的合同法问题是双重的。第一类合同关系调整的是诸如林登实验室（Linden Labs）和动视暴雪（Activision Blizzard）等平台提供商和其用户之间的法律关系。此类合同出现在平台提供商提供的服务或使用条款（terms of services or uses）和最终用户许可协议（end users licensing agreement）中。不幸的是，这些合同中没有最低限度的条款来保护元宇宙用户。例如，法院对用户能否保留其合法权利的裁判不一，这会使事情变得复杂化，尤其是在发生争议时。如此一来，对于同时横跨多个元宇宙平台的用户来说，不存在一致性待遇。

第二类合同关系调整平台用户之间的交互关系。由于元宇宙对任何个人（包括企业）同样开放，因此该类合同可能是 C2C、C2B 或 B2B。与此同时，虽然某项法律能够适用于现实世界的情形，但它在元宇宙中适用的结果可能是不确定的。消费者保护法就是这样的一个例子。因此，元宇宙用户之间的合同关系是独特的，需要在适用特定法律之前逐案分解。

进一步的问题涉及智能合约。元宇宙本质上是一个计算机程序，因此，它通过计算机代码的使用而获得发展，也就必然鼓励智能合约的应用。在元宇宙中使用智能合约可以提升整个元宇宙运行的实用性、效率性和敏捷性，因此，没有必要将传统合同照搬适用于元宇宙中的每一个行为。

（四）网络安全和网络攻击

最近，越来越多的网络攻击发生在虚拟世界中。网络安全的风险随着下一互联网——元宇宙——的展开而有所增加。此类风险各不相同，从身份盗窃到安全漏洞造成的经济损失，不一而足。元宇宙安全问题的关键点包括：（1）身份管理，元宇宙平台提供商如何设计和加强元宇宙用户身份管理的安全性；（2）DDoS 攻击；（3）设备漏洞，这更多的是在用户端；（4）数据外溢和数据开发。一旦发生违规行为，由于有限的补救程序以及管辖范围/地区问题，元宇宙用户是最

〔11〕 例如，游戏《第二人生》平均每天有 20 万的活跃用户，他们来自 200 多个国家和地区。

为脆弱的。

（五）货币和支付系统法

货币和支付系统法的主要法律渊源是两大类法律：货币法和中央银行法。第一类法律为货币作为法定货币的使用奠定了基础，第二类法律赋予了中央银行在其管辖范围内采取货币政策并规范、监督支付系统的权力。〔12〕

大多数国家的货币法将自己的货币定义为法定货币。公民必须使用和接受这种货币来履行金融义务，包括清偿债务。一些国家限制使用其他货币或资产来履行这些义务，而另一些国家则在明确规定使用其他货币或资产方面处于真空状态。这就是为什么当加密货币的使用出现时，各国政府采取了截然不同的方法。美国和中国政府从一开始就明确限制在其管辖范围内使用加密货币。同样的，印度尼西亚政府也禁止使用加密货币作为支付手段。

现代中央银行法更加标准化。它们主要包括中央银行的目标以及法律赋予中央银行实现这些目标的职能或权力。然而，这些目标可以是单一的、双重的，甚至是多重的，具体取决于国家在建立中央银行时的经济、社会和政治条件。无论出于什么样的条件，世界上每一部中央银行法都将维持物价稳定的目标反映在稳定的通货膨胀和汇率上。

由于中央银行的主要目标与维持物价稳定有关，加密货币的兴起就对中央银行的有效性构成了威胁。这是因为，加密货币是由中央银行管辖范围以外的各方或团体发行、流通的私人货币。加密货币的广泛使用将使中央银行的工作变得困难，尤其是在控制货币供应方面。不幸的是，元宇宙中的行为与加密货币、非同质通证以及中央银行以外的私人发行的代币紧密相关。因此，元宇宙的兴起可能会对中央银行履行职责构成更大的威胁。

（六）虚拟资产法规

在货币和支付系统法律的相关问题之后，讨论虚拟资产法规也是很重要的。不同的经济体在监管虚拟资产方面采取了不同的方法。相关的法规包括对加密货币交易要求获得政府许可的证券法、将加密资产视为大宗商品的大宗商品法，〔13〕以及反洗钱法和了解客户规则，〔14〕其要求虚拟财产交易所履行某些义务，如提交可疑交易报告。由于元宇宙仅将加密资产用于其交易，因此不同法律的适用可能导致元宇宙的发展变得复杂。

（七）税法

对虚拟商品和服务以及虚拟世界中的行为进行征税的问题，一直是G20经济体领导人关注的重点。〔15〕事实上，十年前就已经出现了这一问题，即政府是否可以对虚拟世界中的商品、服务和商业交易行为征税。因此，政府需要制定履行此类义务的框架和标准，从而避免双重征税，加重公民、企业的负担。这场运动的主要背景是，虚拟世界一直被视为避税天堂。此外，元宇宙与

〔12〕 对于中央银行法，国际货币基金组织（IMF）有一个由世界上大多数国家的中央银行法组成的数据库，即中央银行法数据库（CBLD）。该数据库可以通过预先查询和注册获取。

〔13〕 例如，印度尼西亚是将加密货币等虚拟资产视为商品的国家之一。

〔14〕 适用此类规则的司法管辖区包括美国、英国、加拿大和德国。

〔15〕 现在，它甚至已经成为G20峰会的主要优先议程之一。G20是一个由20个主要国家和地区组成的合作小组，其中包括美国、加拿大、欧盟、澳大利亚、德国、法国、意大利、沙特阿拉伯和印度尼西亚。今年，在印度尼西亚担任轮值主席国期间，G20峰会进一步讨论了将税收义务适用于虚拟世界中的行为的标准和框架。

区块链紧密相关，而区块链的支付系统是加密货币，这种加密货币以逃税而闻名。元宇宙中的经济交易量不断增加，各方继续享受虚拟世界中的商品和服务，而政府却难以征税。税务机关一直无法触及价值数万亿美元的虚拟市场。

（八）赌博监管

当美国政府禁止《第二人生》这款游戏的赌博功能时，《第二人生》就失去了名气和大量用户。最受欢迎的早期元宇宙版本的用户量减少了近一半，《第二人生》游戏的人气开始下降。最近，《第二人生》的日活跃用户平均为 20 万，来自约 200 个国家和地区。〔16〕

从游戏《第二人生》的案例来看，政府对赌博的监管显然与元宇宙的发展有关。尽管元宇宙声称是一个使用化身进行交互的纯粹虚拟世界，但事实证明，政府在现实世界中的执法会影响元宇宙的存续。因此，元宇宙的倡导者在制定这方面的规则时需要更加谨慎。

（九）刑法

从更加科学的方式出发，我们可以从劳埃·克里斯汀（Laue Christian）提出的三种不同观点来理解元宇宙。第一种观点考虑虚拟世界平台是否会为已有互联网犯罪带来新的维度。也就是说，目前互联网上的犯罪类型有增加的潜在危险，但对于一种全新犯罪类型的发展来说，可能性仍很低。第二种观点将虚拟世界视为一个独立的社会。在这种观点的理解下，犯罪行为的影响可以通过犯罪学来评估。然而，应用这种观点存在一个关键问题，即现实世界中犯罪学的结论往往难以应用于元宇宙的独特条件。第三种观点认为，元宇宙的使用可以触发现实世界用户的反馈效应。这种观点认为长期沉溺于元宇宙会对现实世界用户的行为产生不利影响。然而，这种观点目前来看相当荒谬，因此还需要进一步研究。

有观点认为，元宇宙中的潜在犯罪活动包括跟踪、攻击和虐待行为、儿童色情、绑架、侵犯知识产权以及庞氏骗局等金融欺诈和各种诈骗。运用上述劳埃·克里斯汀的理论，是很难评估这些潜在的犯罪行为的。元宇宙中的这些犯罪是完全新型的犯罪，还是与现实世界的犯罪相似但又独立的类型，可以适用现有的犯罪学理论吗？对此，主张适用现有犯罪学的观点似乎更为便利。如此一来，执法机构就能够简单地使用既有的完备程序来履行其职责。然而，简单粗暴地应用这种观点而不接受任何其他可能的观点是危险的。未来是未知的，元宇宙的发展仍处于早期阶段。因此，元宇宙鼓励思想的开放。

（十）其他问题：治理和伦理

长期以来，人们一直认为虚拟世界缺乏治理。当然，元宇宙也不例外。适用于此类虚拟世界的规则，主要包括使用条款和平台提供商制定的社区标准/规范。事实上，虚拟世界中没有任何民主可言。这是因为，平台掌控者就像独裁者一样统治他们的元宇宙。一些案例已经充分证明，这些平台掌控者往往无法将“社会福利”作为一项优先考虑的事项，因为他们有着私人的商业利益。正因如此，对元宇宙进行标准化的全球治理的呼声应运而生。

另一方面，元宇宙中的伦理问题并不比治理问题更为简单。自从使用 Web 2.0 以来，元宇宙中的伦理问题就被提了出来，然后随着物联网的普遍使用而进一步扩展。在元宇宙中，至少有五

〔16〕 这一数据是由林登实验室（Linden Labs）在 2021 年 6 月 23 日庆祝《第二人生》上线十八周年时公布的。

种与伦理问题相关的场景。它们包括身份问题、不同用户或用户群体的不同伦理和价值观、剥削风险、骚扰和破坏以及犯罪问题。

尽管有人可能会提出元宇宙伦理问题是否重要的问题，但如果我们希望元宇宙得到蓬勃发展，就必须解决这些伦理问题。例如，与身份相关的问题就与元宇宙用户的动机密切相关。接近43%的用户加入元宇宙，是为了通过了解真实的自我来帮助自己。曾经有一项调查显示，75%使用男性头像的用户实际上是女性，而80%使用女性头像的用户竟然是男性。尽管元宇宙是模仿现实世界中的活动，但事实证明，元宇宙中的化身并不是100%代表现实世界中的真人。当然，这种情况会使事情复杂化，尤其是在涉及法律权利和义务时。

四、结　论

虚拟世界、元宇宙的兴起似乎是不可避免的。许多人支持元宇宙的发展，因为它蕴含着巨大的潜力。他们认为元宇宙是继互联网之后的下一个大事件，并将其称为Web 3.0。然而，也有不少人对元宇宙不抱有太乐观的看法，主要原因有以下两个：(1) 元宇宙的想法并不是全新的；(2) 元宇宙的早期版本（例如游戏《第二人生》）并没有很成功，而它当前的版本（例如Sandbox和Decentraland）仍在开发中。因此，这些反对者认为元宇宙的兴起只不过是人为炒作而已。

从法律的角度来看，元宇宙引发了一系列法律难题。关于技术对于法律权威和尊重法律的要求的三种冲击的理论观点表明，元宇宙属于技术冲击的第一种。元宇宙创造了一个现实世界中的法律可能难以适用的空间。因此，元宇宙破坏了法律权威的“传统主张”，以及仅仅因为它是法律而尊重法律的要求。然而，将现实世界的法律适用于元宇宙中的行为是最简单的方法，尽管这种方法并非没有挑战。尽管元宇宙中的行为被认为是在模仿现实世界的行为，但将现实世界的法律适用于元宇宙中存在很多局限性。

第一个局限涉及元宇宙的财产及其所应适用的所有权框架。物权法很难在元宇宙中适用，因为元宇宙中的财产不是物权法所调整的具有物理性存在的有体物。知识产权法可能更适合在元宇宙中适用，但法律管辖、法律选择和法律执行等问题也会出现。这样的法律在纸面上对于元宇宙来说可能是完美的，但在具体实施中将是有缺陷的或者不完整的。进一步的难题涉及：(1) 元宇宙存储和管理大量数据（包括用户的个人数据）所带来的数据保护问题，以及跨界数据流动问题，因为元宇宙中的用户通常来自数百个国家；(2) 如何在元宇宙中适用“传统”合同法，因为元宇宙主要使用智能合约来实现其整体运作的实用性、效率性和敏捷性；(3) 网络安全问题，因为越来越多的网络攻击发生在虚拟世界中；(4) 各国政府对虚拟商品、服务和商业行为征税的共同努力；(5) 政府限制元宇宙中的赌博活动，对元宇宙的发展产生了不利影响；(6) 将刑法适用于虚拟犯罪的问题；(7) 元宇宙被指责缺乏治理和民主，并且元宇宙的一些用户在行为上缺乏道德感。

此外，需要特别强调的是将货币和支付系统法适用于元宇宙的局限性。货币和支付系统法的法律渊源是货币法和中央银行法。这两类法律都倾向于限制加密货币在元宇宙中的使用，因为加

密货币给中央银行实现维持物价稳定的目标带来了困难。美国、中国和土耳其等国家都采取了在管辖区范围内限制使用加密货币的方法。此外，加密资产的法规因不同司法管辖区而异，这也对元宇宙的繁荣构成了障碍。此类法规包括美国的证券法、印度尼西亚的大宗商品法以及英国、加拿大和德国适用的反洗钱法和了解客户规则。

Abstract: The metaverse has gained momentum after the CEO of the biggest social media organization made a statement that the metaverse would be the next big thing after the Internet. Although there is no single, agreed upon definition of the metaverse, the common understanding of the metaverse is that the concept combines IoT, AR, VR, XR, and 3D technologies. The market capital and other economic potential of the metaverse is enormous. Hence, it is of importance to discuss the legal implications of the metaverse. This article is the first to elaborate the legal conundrums of the metaverse in a proper manner. It includes discussion of general and property law and intellectual property law, and whether the time has come to have "a virtual property law". It also discusses some other legal issues such as privacy and data protection, contract law, cybersecurity and cyberattacks, monetary and payment systems laws, and regulation of virtual assets, tax law, anti-money laundering laws and KYC, and criminal law. The metaverse creates a space where the law of the real world may be difficult to apply. Therefore, the metaverse disrupts the "traditional claims" from the legal authority and the demand for respect for the rule of law just because it is the law. However, applying this subset of the real-world laws to the metaverse turns out to be possible, but with limitations. Such limitations arise specifically when it comes to the operation of the law.

Key Words: metaverse, legal conundrums, virtual world, monetary law, payment system law

(责任编辑：张金平　赵建蕊)

财经法学 No. 4，2021
pp. 3 - 22

社会信用建构：基于大数据征信治理的探究

黎四奇*

内容提要：社会信用是社会秩序维系、人际关系和谐、交易规范与拓展、民富国强的基础，其对于构建社会主体命运共同体具有时代性的意义。大数据正以其技术性特质改变着传统征信模式、方法与观念，对征信治理的推陈出新产生诱导性的进化效应。大数据时代，大数据征信以其技术优势推动与加速社会信用的建构，促成信用国家的形成。法律是社会利益的调节器与社会秩序的稳定器，当征信治理制度滞后于社会信用发展的需求及科技的进步而衍生供求矛盾时，从目标定向、理念明确、利益保护平衡、市场安全及尊重互联网精神等角度进行法律的因时与因势而进就是一种理性选择。

关键词：社会信用　大数据征信　信用中国

为了实现“信用社会”这一宏伟目标，我国推出了一系列纲领性文件，如 2014 年 6 月的《社会信用体系建设规划纲要（2014—2020）》（以下简称为《信用纲要》）、2019 年的《关于加快推进社会信用体系建设构建以信用为基础的新型监管机制的指导意见》。虽然信用社会的形成不可避免地依存于传统、风俗与制度等，但是其更应通过对社会主体行为进行评价的方式得以落实。在前大数据〔1〕时代，囿于互动应景与技术等原因，与社会主体相关的信用信息呈现出破碎化、零散化的特点。让数据“发声”的大数据技术开启了重大的信用评价转型。研讨大数据征信治理对社会信用建构具有举足轻重的作用。

* 黎四奇，湖南大学法学院教授。

〔1〕“数据”与“信息”是两个相互联系的概念，数据本身就是信息，是信息具体的表现方式。信息经过数字化处理后才能复制、存储与传输。对此，我国《网络安全法》第 76 条第（四）项规定：“网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。”

一、社会信用建构的机遇与挑战：大数据征信

（一）大数据征信的识别

信用国民、信用社会、信用国家是我们孜孜以求的目标。当大数据与征信相结合时，它标志着大数据征信已在事实上开启一个国家诚信建构的新模式与新时代。概念是人类认识和把握世界的重要手段。为了廓清“大数据征信”这一关键词，研究者进行了诸多解释。“大数据征信是指将大数据技术运用于征信活动，通过采集、分析、挖掘多维度的海量数据信息，并借助机器学习等模型算法来描述信息主体的信用状况，为多样化的应用场景提供征信产品。”〔2〕“大数据征信是指基于大数据技术设计征信评价模型和算法，通过多维度的信用信息考察，形成对个人、社会团体、企业的信用评价。”〔3〕“大数据征信从其本质上来看，是将大数据应用到征信活动中，突出强调的是处理数据的数据量大、刻画信用的维度广、信用状况的动态呈现、交互性等特点。”〔4〕

在结构上，大数据征信即“大数据”与“征信”的结合，它意味着大数据对传统征信的渗透与影响，如在信息上，强调总体性，而非局部性，强调信息之间的相关性，而非因果性。客观上，“征信以采集、保存、分析大量的信息为主，大数据技术为征信提供了一种全新的数据处理模式”〔5〕。由于大数据与互联网之间密不可分的关联，在研究中，亦有人使用了“互联网征信”这一概念，并将其界定为“采集个人或企业的互联网信息数据，并结合线下渠道采集的信息，使用大数据、云计算等技术来评估信用的活动”〔6〕。

大数据征信与互联网征信实为一个问题的两个方面，前者突出的是数据的收集、整合与分析能力，后者强调平台与数据的传输能力。由于数据流动于网络之间，若我们拟对大数据征信有个全面、客观、科学的理解，就必须立于技术的层面对互联网有个基本的认知。互联网是一个由不同类型和规模、独立运行和管理的计算机组成的集合性网络。互联网的关键在于“联”，它表明任何人、任何事物、任何时间与任何地点的实时在线与实时联动。正由于“互＋联＋网”的特性，人们将互联网精神凝练为开放、平等、协作与共享，而这也决定了与传统征信相比，以网络为依托的大数据征信具有以下新的技术特征。

1. 征信数据的广泛性

社会信用是一项体系性的工程，它张扬的是，一处失信，则处处受限，即“意味着失信人在一处出现失信行为，就会处处受到限制”〔7〕。为了确保社会中的每个人都能坐言起行与言而有信，征信数据多多益善。由于分析技术及数据源狭窄等原因，传统征信难以全面有效覆盖。当下，互联网、移动智能终端的普及和大数据挖掘技术的发展已使这一难题迎刃而解，大数据征信

〔2〕 陈小梅：《我国大数据征信业发展实践与完善路径》，载《福建金融》2017 年 12 期，第 59 页。
〔3〕 刘晓：《我国大数据征信个人敏感数据保护困境及保护机制研究》，载《西南金融》2019 年第 1 期，第 30 页。
〔4〕 孔德超：《大数据征信初探——基于个人征信视角》，载《现代管理科学》2016 年第 4 期，第 39 页。
〔5〕 鞠卫华：《大数据征信特点及其风险探析》，载《金融科技时代》2017 年第 2 期，第 30 页。
〔6〕 余丽霞、郑洁：《大数据背景下我国互联网征信问题研究》，载《金融发展研究》2017 年第 9 期，第 46 页。
〔7〕 沈岿：《社会信用体系建设的法治之道》，载《中国法学》2019 年第 5 期，第 29 页。

的征信对象可以无遗漏地覆盖全部网络使用者。同时，用户行为属性具有多样性，其遗留的数据已全方位地涉及人们物质与精神生活的方方面面。大数据使传统征信正面临一种脱胎换骨式的变革，因为“大数据征信将传统征信的金融借贷扩展到其他的生活场景，从信用主体的消费、出行等行为信息也可推断出其相关的资质和能力，为信用评估提供多角度的评判场景”〔8〕。

2. 征信数据的海量性、低成本性与实时性

大数据的首要特征在于其数据产出量与存储量的巨大。虽然这些数据具有价值低密度性，但是它向人们展现了以下事实：我们正生活于一种不断变化但却日趋被严密监视的状态中。我们的一举一动都可以在某个数据库中找到对应的线索。大数据第一次毫无歧视地为我们每一个人保留了详细的行为记录，而这为信用评价提供了丰富的素材。互联网信息具有实时、全貌及线上与线下相结合的特点，而传统征信的信息来源渠道狭窄、单一，且多以昨天的信用记录对今天的信用状况进行评估。虽然在网络技术的支撑下，大数据征信优势显著，但是其开放、平等、自由等特点也使得征信市场应有的安全、公平、利益平衡等底线价值面临严峻的挑战，如“平台征信数据具有较强的时效性，但同时也会产生大量无用、虚假的信息噪音，而互联网技术并不能从海量的信息中辨别、遴选出真正有用、真实的信息”〔9〕。

3. 数据存储的便捷性与处理的智能性

大数据征信的亮点在于大数据接入、大数据存储、大数据共享与交换、大数据展现及大数据分析与挖掘技术，而这彻底革新了征信的观念与模式，从而极大地推进了社会信用的建设。随着数据技术的发展，数据多以电子邮件、视频、语音、图像等非结构化或半结构化的方式体现，且存储工具与模式日益翻新与多样化。人工智能是大数据的时代技术标签。“随着数据量呈几何级数的增加，征信机构甚至可能并不需要投入硬件来建立实体数据存储设备，而是通过技术创新，形成由大规模计算机集群组成的‘云’存储大数据。”〔10〕

在大数据技术下，智能化的数据平台可自动完成信息生成、传送、收集、整理、加工、分析等一整套工序，平台多具有强大的信息捕捉、组织、排序与检索功能，可低成本、高效率地满足信用评价的数据需求。更重要的是，借助大数据与云计算，还可将大量破碎、难以量化的“软信息”提炼为可以进行信用识别与定性的“硬信息”。

4. 征信数据使用范围的宽广性

这主要表现在以下几个方面：一是信用评价趋于生活化与常态化。在用途上，不再局限于传统的银行信贷融资，而被广泛地应用于网购、住宿、医疗、出行等日常活动。二是被用于网络借贷的资信评估。为了控制信用额度与风险，一些网贷企业通过自身的数据征集对借款人的信用度进行考评，如“芝麻信用”就从客户的信用历史、履约能力、行为偏好、身份特色和人际关系五个方面来采集信息，以作为发放贷款的重要条件。三是应用于学术评价，遏制学术不端行为。庞大的数据库可以集中海量的学术成果，数据查重系统可以提供学术信用评价。四是为社会治理提供有力

〔8〕 贾拓：《大数据对征信体系的影响与实践研究》，载《征信》2018 年第 4 期，第 19 页。

〔9〕 陈小林：《我国互联网金融征信体制建设路径思考》，载《征信》2015 年第 1 期，第 29 页。

〔10〕 戈志武：《大数据征信监管研究》，载《西南金融》2017 年第 4 期，第 14 页。

的数据支持。信息的占有量、种类及定性分析等直接关系到政府对行为人行为模式、遵纪守法性的预判，这可以极大地提升社会治理效率，降低治理成本及对风险进行事前防控。

（二）亟待解构的法律治理问题

大数据征信不仅意味着社会信用与价值在互联网、云计算、人工智能等技术激励下的放大与升级，更意味着一种利益的重置与法律的革新。在探究社会信用法律治理改良时，在顶层设计上，以下问题应纳入深思的范畴。

1. 数据特性的协调

大数据给征信创新提供了历史机遇，但是人们依然对以下问题心怀忧虑：这些数据能否全部用于征信、如何确保数据的客观性与准确性、如何防范大数据的黑箱操作等。大数据、网络与云计算是大数据征信的基础，但是如果我们致力于将这种方式融入法律化的生活，那么就不得不面临以下现实："执迷于精确性是信息缺乏时代和模拟时代的产物。只有 5％的数据是结构化且能适用于传统数据库的。如果不接受混乱，剩下 95％的非结构化数据都无法被利用，只有接受不精准性，我们才能打开一扇从未涉足的世界的窗户。"〔11〕

"传统的信用评价模式主要是关注、分析考察对象的历史信息，数据少且时效性差，而大数据征信将注意力从数据的精确性转移到数据的相关性上。"〔12〕因此，有人认为，大数据无法消除不确定性，而不确定性即意味着风险。如果由于大数据的零碎、"噪音"等缺陷而在征信观念、模式上裹足不前，那么不仅会导致社会信用评价资源的浪费，而且自限的做法也会抑制新事物的萌芽与成长。实际上，大数据征信面临两种可能性：一是丰富与多元的信息使信用评价结果更加客观、科学与公正；二是信息"噪音"或"脏度"过大影响评价结果的精确性。大数据时代，虽然人们可获取的信息量巨大，但是低劣、虚假、失真的信息也混杂其中，数据漏报、错报、假报等现象也频频发生。数据是征信机构的重要资产，为其安身立命之本。信用国家建构中，确保征信数据的真实性、关联性与完整性应是关注的重点。

2. 利益平衡下的安全保障

大数据技术的迅猛发展正在日益刷新人与人、人与社会、人与自然之间的关联模式，使传统法律秩序遭受巨大的挑战，如信息传递、采集的广度、深度、速度等特质使得信息越来越公开与透明，而这进一步使得隐私权保护变得举步维艰。当人类共同体的利益与安全受到威胁与冲击时，借助法律的方式寻求妥协与平衡就成为必然。在社会善治中，法律被寄寓了平等、自由等多种理想元素，但安全是其他价值的基础。与传统征信相比，大数据征信使得数据安全问题更加突出，这主要表现为：数据的过度采集会干扰人们的日常生活，无度挖掘会深度触及公民的隐私或企业的商业秘密，计算机网络系统的故障、黑客攻击与无处不在的木马程序等使消费群体的金融与隐私数据时刻面临可能的外泄风险。

法律治理的目的不是自由，而是安全与平等。虽然大数据革新了征信模式，但是若不能通过法律治理给予民众网络信息的安全感，那么很有可能我们会为其发展付出更多的成本。信用国家

〔11〕〔英〕肯尼思·库克耶等：《大数据时代——生活、工作与思维的大变革》，盛杨燕等译，浙江人民出版社 2013 年版，第 45 页

〔12〕 植凤寅：《大数据征信与小微金融服务》，载《中国金融》2014 年第 12 期，第 91 页。

建构中，作为公民，我们有义务让社会了解我们的信用记录，但我们的隐私权与数据安全权也理应得到社会的尊重。然而，我们不得不面对一个困境，即数据保护与隐私权是否为同一概念，或者说隐私权保护本身是否包括了数据保护。“作为一种价值，隐私是一个非常复杂、既相互配合又自相矛盾的概念，它被塞满了各式各样确切的意图。如果想将之彻底解决，这是件令人沮丧的事情。”〔13〕

法律为善良与正义的艺术，事关和谐与统一。在时下的法律体系中，人们惯于从因果关系的角度来理解行为、责任、权利与义务之间应有的正义关联。然而，当大数据盛行及大数据与征信结合时，这一熟知的“公理”将会被打破。大数据预测与信用评价下，在社会治理中，行为人将不是因为做了什么而受到惩罚，相反，是因为将要做什么而受到惩罚。理性而言，基于未来可能行为的惩罚是对正义的亵渎，因为正义的基本逻辑是，行为人只对其所作为承担责任。虽然大数据预测为我们打造一个更安全、更和谐、更有秩序的社会提供了技术支撑，但也否定了我们人之为人的一个重要价值，即自由选择与责任自负的能力。当大数据及大数据征信成为集体选择的工具时，我们也不得不弱化或放弃意志的自由。法律是利益固化与风尚引领的方向标，大数据征信治理中，利益如何平衡也是法律必须厘定的问题。

3. 数据共享与利益冲突

虽然网络技术的发展推进了信息传播、搜集与共享，但是其仍不足以为大数据征信提供全面的支撑。当下，底层数据缺乏，如日常的教育、住房、社保、医疗、学术诚信等基础数据尚未完全并网，社交数据与支付数据等亦相互闭锁，“信息孤岛”现象严重阻滞了社会信用的建构。征信意在从社会整体上防范与惩戒失信。然而，大数据征信却落入了一个故步自封的陷阱，这不仅是对互联网共享、协作精神的背离，而且私利驱动下的“自我封锁”也必然造成大数据征信行业标准的缺失与征信资源的浪费。行业标准的缺失会引发以下连锁性反应：各大数据征信平台推出自设的征信标准→类似的数据在不同的征信平台形成截然不同的评价结果→消费者受到不公正待遇→恶性竞争→市场紊乱→社会信用受挫。

本义上，征信特指为了弱化或消除信息不对称现象，专业的第三方机构依法采集、存储、整理与加工有关自然人、法人等的信用信息，并以此为基础，帮助经济主体判断和控制交易风险的信用中介服务活动。因此，专业、中立与公正是对征信业的必然要求。然而，就现实而言，许多大数据征信平台既当“裁判员”，又当“运动员”。如“阿里巴巴办理征信的天生缺陷就是不具备独立于金融交易双方的第三方资质，一个企业不能既从事金融交易，也做征信”〔14〕。京东亦顺手将京东商城海量的消费数据作为信用评价的依据，以向客户营销其金融信用产品。

4. 立法模式选择

在研讨大数据征信中，有必要辨识其与传统征信的异同，因为这直接涉及法律体系的分类建设。在追求法律的科学性与严密性中，立法者往往将人、物与行为归于一定的类别，并依据共同的标准对其进行调整。就法律治理而言，如果大数据征信与传统征信具有高度的同质性，那么理

〔13〕 Post，Robert C.，Three Concepts of Privacy，89 *The Georgetown Law Journal*，2087－2098（2001）.

〔14〕 刘新海：《阿里巴巴集团的大数据战略与征信实践》，载《征信》2014 年第 10 期，第 12 页。

所当然地，其应属于同一个法律体系，而无须分置立法。反之，则不然。实质上，大数据征信只是征信技术、方法与模式等的改变，其传统的以社会信用为目标的征信功能与价值并没有改变，更贴切地说，大数据征信只是数字技术支撑下传统征信的更新换代。

（三）社会信用建构：大数据征信治理的目标

“无物不互联、无处不数据”的大数据时代，征信业务大数据化已是大势所趋。在这种浪潮下，一些原有的征信机构也主动开始转型，如北京安融惠众征信、北京宜信至诚信用评估等。此外，腾讯、京东等互联网企业也嗅到了这一商机，这些新动向必然会推动征信业法律治理的变迁。任何一种制度与理论都应是针对某个特定时代的问题所作出的一种经验性回应。现实是，大数据正在润物细无声地创新人类的思维方式，使我们的思维模式从串联性的因果关系向并联性的相关关系发展，使我们的物质与精神生活立于数据之上。凡物皆可数、数据人、数据资产已成为我们这个时代的特征。

法律是人类生活经验与理性的浓缩，代表一个社会最具有权威性的价值准则。网络化的大数据征信不仅使原局限于银行征信数据的时代一去不返，而且也彻底革新了传统征信的理念，因为它“强调一切数据皆为信用、所有信息看关联不看因果、错的信息也是关键信息”〔15〕。在法律还没有及时介入时，逐利性使得大数据征信在电子商务、网络社交平台等的推动下获得蓬勃发展。当法律演进滞后于技术创新时，由于法律体系外的漏洞，现时的征信制度不可能对大数据征信从一个“入市→运营→退出”的生命周期作出事无巨细的安排。然而，这并不表明，在互联网精神的统摄下，这一领域就成了一个绝对自由、可随意侵犯他人隐私、侵蚀国家主权的“飞地”。人民的安全是至高无上的法律。在信息的攫取、占有等几乎无孔不入的情况下，或许这句格言能指引我们信用法律治理前进的方向。

大数据技术使人类正处于一个变动不居的世界中，而这使得社会信用建设尤为紧迫。“世界的变化与突发事件使得人们无论行动与否都处在一种风险之中，风险是不可回避的。人们化解或预防风险之道在于信任，由于熟悉导致的信任变得有限，社会需要一种系统信任，即制度化的信用。”〔16〕虽然我们日渐接受了法律理性的论断，但是又不得不承认作为理性产物的法律还与人类的经验紧密相关，而这也是大数据征信治理必须考虑的问题。大数据并不完美，在有关大数据征信的不同观点之间的针锋对垒中，法律治理之路究竟该何去何从？在法律的勾勒中，大数据征信是作为外在经验而存在的，如果立法者的意图是拟配置与其相适的法律规则，以引领、规范、保障其发展，从而促进信用社会与信用国家的建构，那么从“问题是什么→法律是什么”的角度来审视就是一个事半功倍的研究方法。

二、社会信用建构的瓶颈：我国征信治理存在的问题解析

（一）宏观上的短板：应有法律理念的缺位

在人类的繁衍与发展中，功利主义对人们行为的选择总是充满着难以抗拒的诱惑力。受利益

〔15〕 刘旭、赵玉清：《大数据环境下互联网征信发展与监管研究》，载《河北金融》2016 年第 4 期，第 6 页。

〔16〕〔英〕安东尼·吉登斯：《现代性的后果》，田禾译，译林出版社 2000 年版，第 6－8 页。

的驱使，在法律的进化中，它也直接左右了法律人的方法论，使人们更多不是从最先的事物、原则、范畴和假定是必需的东西出发，而是将最后的事物、收获、效果作为选择的标准。虽然目的正当决定手段正当提高了制度创制的效率，但是还必须深刻地认识到，功利性的法律还必须接受理念的监督与守望。“法律是按照其意义必须服务于法律理念之物。”〔17〕我国征信法律治理起步相对较晚，在理念体现与贯彻方面，其仍存在以下值得深思之处。

1. 立法缺乏前瞻性

法律必须时刻具备成长的原则，这决定了法律必须紧跟时代发展的诉求。我国征信法律制度的建设也只是近几年来的事情，如较早的《征信业管理条例》便诞生于 2013 年 1 月。同期，一些大数据征信平台也应景而生，如上海资信旗下的“互联网金融征信”（NFCS）推出于 2013 年 6 月，“安融惠众信用信息共享平台”（MSP）于 2013 年 3 月正式上线。这种状况表明，我国的征信制度构建与大数据征信之间并不存在明显的时差。然而，纵观这些规范文件，我们难以从其字里行间里捕捉到与大数据征信直接相关的内容。

大数据语境下，“大数据既是一种资源，也是一种分析、预测工具，可以将过去难以计算、存储、分析、共享的事物变得有利用价值，并可预测未来，帮助人们认识世界”〔18〕。大数据为社会信用度量提供了一个全新的广角，基于充沛、多途径、交叉互补的数据，征信机构可以将行为人多属性的零碎性的信息串联起来。“虽然征信活动的实质和征信业务开展的原则并不发生根本性的改变，但是大数据征信改变了数据采集、整理、保存、加工、提供的方式和手段。”〔19〕尽管大数据征信与传统征信存在源流关系，但是大数据征信却会带来一系列破局性的改变，如数据特质、征信理念、征信方式、征信内容、评价方式，甚至评价结论都会发生根本性的变化。法律的与时俱进、法律先于立法说明理性的立法必须为明天时刻准备着。客观而言，新技术应景下，未来性思考的缺失是我国时下征信法律治理应着力解决的瑕疵。

2. 法律问题政策化与道德化

为了践行社会信用体系与巩固诚信的社会价值观，近年来我国推出了一些纲举目张的政策性文件。虽然这些文件是我国社会信用建设的方向标，但是“建设法治化的社会信用体系，需要统一的信用立法，划定社会信用制度的规则界限”〔20〕。依法治市中，“信用不再仅是道德约束或法律解释的对象，而是须通过具有权威性、可量化、可公开的信息来表征的特定主体的守法或履约状态”〔21〕。依法治国代表了认识大同，以法律的方式，而非政策或道德的方式就是我国征信法律治理前进的路标。

民无信不立，业无信不兴，国无信则衰。虽然道德的教化能塑造与固化人们的诚信观念，使人修身正行，但是人自利的劣根性决定了诚信的确立与维护更是一个刚性的法律制度建构问题。“法律反映或符合一定道德的要求，尽管事实上往往如此，然而不是一个必然的真理。”〔22〕以法

〔17〕〔德〕拉德布鲁赫：《法哲学》，王朴译，法律出版社 2005 年版，第 73 页。

〔18〕连镇殿等：《大数据背景下城市公共信用信息平台建设研究》，载《宏观经济管理》2017 年第 2 期，第 61 页。

〔19〕宋媚：《大数据征信背景下的信息质量度量与提升研究》，上海交通大学出版社 2016 年版，第 8 页。

〔20〕李林芳、徐亚文：《社会信用体系法治化原理探析》，载《学习与实践》2019 年第 11 期，第 29 页。

〔21〕王瑞雪：《政府规制中的信用工具研究》，载《中国法学》2017 年第 4 期，第 159 页。

〔22〕〔英〕哈特：《法律的概念》，张文显译，中国大百科全书出版社 1996 年版，第 181－182 页。

律，而不是纯以道德来强化诚信有助于人们认清法律组织性的权威与强制，并可防止法在“应该这样的”道德评判中化为乌有。“鉴于信用立法是社会信用体系建设的关键环节，因此将政府赋能的社会信用体系建设模式，转变为以法赋能的社会信用建设模式，是新时代社会信用体系建设进一步快速发展的关键。”〔23〕客观上，将诚信建设拉回法治的轨道，无论其是否存在这样或那样的缺陷，这本身就是正义的宣告与胜利。大数据之下，如果我们以信用为核心的征信治理是一个历史、进化的命题，那么它的完善、精致或拙劣等都必须接受“肯定即否定”的检讨。

3. 欠缺体系性

体系即依一定的原则所构成的知识整体，意味着周密、逻辑、整体与一致，是衡量人类对客观事物的认知是否科学的重要标杆。自不待言，征信是一个体系性的系统，“征信体系是指采集、加工和分析信用信息并对外提供信用信息服务的相关制度和措施的总称，包括征信制度、征信标准、信息采集、征信机构和信息市场、征信产品和服务、征信监管等”〔24〕。这种阐释表明在征信治理法律制度的构造上，其应该是一个内部条理清晰、结构严谨的系统，而不应是一个由数个单行文本组合而成的零散体系。

市场需要信息交换，没有信息交换的市场是不存在的。因此，征信法治化对我国向市场与法治国家转型的意义是不证自明的。自 2009 年以来，我国紧锣密鼓地出台了《征信业管理条例》《征信机构管理办法》等文件。遗憾的是，从这种“碎片”式的规范文本制作中，很难得出我国征信法律治理体系化建设的结论。哲理上，人不能两次踏进同一条河流，但是文件名称措辞高度雷同的《征信机构监管指引》与《征信机构管理办法》再次给人一种“踏进同一条河流”的感觉。虽然这些规范文件起到了短平快的应急效果，但是其急功近利与短视也使得我国在征信法律治理的建构上与法律应有的体系性渐行渐远。

在法律制度的创制中，我国立法呈现出浓厚的功利性。虽然在这一思想的宰制下，我国已快速地创建了特色性的信用规范体系，但是规则之间的不一致性、上位法粗放性以致必须依赖下位法或解释来救急等弊端也彰而不隐。作为“冰山的一角”，我国征信法律制度不可避免地存在功利主义的痕迹，如《征信业管理条例》理应顺势基于大数据背景对体系中所涉的征信产品、征信机构、信息采集与使用等规定得面面俱到，但是该条例包括附则在内也只有简单的 47 个条文。也正是由于条文过于单薄，2013 年 11 月中国人民银行推出《征信机构管理办法》，2015 年 10 月又发布《征信机构监管指引》。如此高频的“打补丁”不仅人为地打破了征信制度应有的体系，而且也导致监管权威、治理效果与规则确信的边际效应递减。法律并不是由一个个孤零的条文汇成的综合体，而是作为一个整体性的过程、事业、生活方式而存在。否则，现实存在的法律，只是徒有形式的躯体。

（二）微观上的缺憾：大数据征信具体指引上的难点

大数据已从社交、医疗、支付、电商等多个角度嵌入人们的生活，使人类的生活网络化与数据化。虽然法律必须具有恢宏的灵魂，但是其毕竟又要以一种服务于人类生活细节的方式存在。

〔23〕 谢新水、吴芸：《新时代社会信用体系建设：从政府赋能走向法的赋能》，载《中国行政管理》2019 年第 7 期，第 34 页。
〔24〕 唐明琴等主编：《征信理论与实务》，中国金融出版社 2015 年版，第 16 页。

在这一点上，既存的征信制度与大数据之间接轨的不畅使得许多细节问题还没有被纳入治理的范畴。同时，法律侧重稳定性与大数据动态性之间的反差也使得有些法律不是作为大数据征信的激励因素，而是作为制约因素存在。

1. 大数据征信平台的市场准入问题

虽然在市场自发力量下，我国已产生了一批大数据征信平台，但是在缺乏准入许可的情况下，这些平台面临适法性问题。2015 年 1 月 5 日，中国人民银行印发了《关于做好个人征信业务准备工作的通知》，要求腾讯征信、芝麻信用、中智诚征信、鹏元征信、拉卡拉信用、北京华道征信、深圳前海征信、中诚信征信八家机构在六个月内做好个人征信业务的准备工作。虽然从该文件，我们可以对大数据征信存在的“合法性”作正面的解读，但它毕竟不是对《征信业管理条例》第 6 条〔25〕核准制的正式松绑。大数据征信是一种创新性业务，在监管者对其合法性没有给予正式认可前，其存在就处于一种适法不明的状态。

此外，“随着数据的积累和扩展，部分企业也有意申请中国人民银行征信牌照，向其他组织、机构有偿提供系统内部数据，开展市场化征信业务”〔26〕。然而，依什么样的标准给大数据征信企业颁发许可证或让传统征信业进行大数据化的提质是一个需要慎重考虑的问题。如果不加分别地适用《征信业管理条例》第 6 条的规定，则可能人为地掩盖或忽视大数据征信平台的特殊性。虽然一脉相承，但是大数据征信毕竟与传统征信有所不同，其特色在于大数据与云计算下信息的互联互通与高效的智能处置。如果从二律背反的思维出发，那么以下可能性就必须引起高度的重视，即“通过互联网采集、传输和提供网络征信服务，容易受到网络黑客和病毒的攻击，一旦出现信用信息被非法访问、截取和篡改，信息系统遭到不可逆转的破坏性影响，将对个人隐私和客户权益保护构成重要威胁，而且网络风险的扩散性和破坏性更大”〔27〕。我国大数据征信刚起步，信息安全体系建设与风险控制经验不足，数据库防护网的大量技术包更是加剧了系统性安全风险。在这一状况下，如果不针对大数据的风险点配置相应的入市条件，则悖于大数据征信应服务于社会信用建构的目标定向。大数据征信最突出的优势是大数据，而这也决定了数据库技术、数据收集、数据处理、数据分析、数据系统安全等是其安身立命之本。因此，除了一般性要求外，数据挖掘技术、数据安全保障、大数据处理能力也应是认证大数据征信必备的资质条件。

2. 数据采集的法律风险

信息的充分获取是大数据征信运作的必要条件。当下，以电商、第三方支付、网络交际等为基础的大数据征信平台多在用户不知悉的情况下采集信息，如“芝麻信用就先利用阿里云业务对搜集的信息进行储存和初步处理，然后对其进行结构化的清洗”〔28〕。如此，就存在违规与侵犯用户权益的法律风险。在用户信息保护上，我国采取的是严格保护主义，如《征信业管理条例》第 13 条即规定：采取个人信息应当经信息主体本人同意，未经同意，不得采集。《网络安全法》第 22 条第 3 款规定：“网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得

〔25〕 该法第 6 条规定，设立经营个人征信业务的企业，必须符合法定的条件，并且经国务院征信业监督管理机构的批准。

〔26〕 方增平：《互联网金融背景下发展新型征信机构的思考》，载《征信》2015 年第 5 期，第 38 页。

〔27〕 黄玺：《互联网金融背景下我国征信业发展的思考》，载《征信》2014 年第 5 期，第 51 页。

〔28〕 李蕾、王雪：《论我国互联网征信业务发展》，载《征信》2016 年第 8 期，第 36 页。

同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。”此外，如果大数据征信机构不经意间采集了宗教信仰、基因、既往病史、存款、商业保险、不动产及纳税额等敏感信息，则违背了《征信业管理条例》第 14 条的禁止性规定；若在征信体系或评估中设立“黑名单”，则涉嫌违反《征信业管理条例》第 15 条的规定，即“信息提供者向征信机构提供个人不良信息，应当事先告知信息主体本人”。

技术使得数据信息可以被物化为书籍、影视作品等，但是同时它又具有非物质性。数据信息能否商品化是一个无定论的问题。“不管怎样，信息无论是在定义上，还是在概念上，均满足不了作为商品所应具备的条件。因此，在人们关注某一危机中，就引入了一个关于信息本身内在根据的学术论题。”〔29〕在已被实然商品化的时下，一个简单而流行的认识是，信息就是能被数字化的一切。既然如此，在信息商品是依存于信息的情况下，基础性的信息究竟属于谁？属于采集人，还是属于信息的制造者（用户）？对此，人们的观点不一。如有人认为：“个人应有权出售自己的信息，并因此会使公司将它们外在化的成本内在化。数据主体将参与数据交易，并可能为隐私自行定价。”〔30〕另有学者则认为：“无论如何，在美国，征信机构确实是数据的所有者，并由此能更自由地使用数据……到目前为止，只有弱小的权力被赋予个人来阻止公司将数据用于营销目的。”〔31〕当下，虽然各大数据征信机构都在几乎零成本地使用用户遗留的数据，但是在法律还没有白纸黑字地确定其权属时，征信业确实整体面临一个“釜底抽薪”的权属争议风险。

3. 信息主体权益保护与征信权利之间的失衡

信用信息共享是一国信用体系构建的核心，是降低信息不对称、遏制欺诈、营造诚信环境的重要手段。互联网时代，“每个人都成为了信息提供者及需求者，各种公私机构都在无时无刻提供并获取信息，而互联网、搜索引擎的检索及查询功能又加速了个人信息的传播、利用及共享”〔32〕。大数据时代，“数据割据、数据孤岛和数据质量是最典型的三大数据治理问题”〔33〕。其中，大数据安全尤为急切，大数据技术能源源不断地为征信机构输送与整理海量的信息，提升了信用评价的效率，但是信息采集的边界与范围日渐模糊，这也导致信息权与数据保护等成为时代焦点。

在表象上，虽然大数据征信导致隐私权衰落与信息不再隐秘，但是信息利用与保护所体现的效率与公平依然是法律中不变的主题。移动支付、网络交际、电子商务、共享经济等与日俱增地加重人类对数字科技的依赖。“无数据，不人权”已成为这个时代的权利诉求。“数字科技必须以人为本，必须把人的利益进而把人的权利作为其最高价值，以人权尺度为其划界，以人权作为评价科技进步的根本标准。”〔34〕在大数据征信体现信息公开的同时，也必须张扬信息的严格保密。否则，在技术与知识的非对称下，就可能滋生肆意采集和泄露信息、监守自盗信息等侵犯信息主体权益的风险。“芝麻信用”就是一个缩影，因为根据不能讨价还价的《芝麻信用服务协议》，用户授权“芝麻信用”采集信息，并同时默示同意在第三方查询非贷款类及其他非涉及商业秘密信

〔29〕 Babe. R. E，*Information and Communication in Economics*，Kluwer Academic Publishers，1994，p. 42.

〔30〕 Samuelson，Privacy as Intellectual Property? 52（5）*Stanford Law Review*，74（2000）.

〔31〕〔德〕尼古拉·杰因茨：《金融隐私——征信制度国际比较》，万存知译，中国金融出版社 2009 年版，第 24－25 页。

〔32〕 张继红：《论我国金融消费者信息权保护的立法完善》，载《法学论坛》2016 年第 6 期，第 93 页。

〔33〕 赵国栋等：《大数据时代的历史机遇：产业变革与数据科学》，清华大学出版社 2013 年版，第 47 页。

〔34〕 张文显：《无数字，不人权》，载《北京日报》2019 年 9 月 2 日，第 15 版。

息时，其可以直接向第三方提供相关信息。大数据征信开启了一个社会信用建构的新时代，但是“信息处理过程的网络化、数字化使得法律监管难以受到有效的监督，成为了法律监管难以企及的法外空间”〔35〕。虽然随着法治国家观念的深入及个体意识的觉醒，我国对个人信息的法律保护已有所建树，但未来仍是长路漫漫。大数据背景下，在个人信息保护上，我国仍存在以下缺陷：

一是所涉法律条文有限、分布零散、适用范围窄，且未体系化。“在个人信息保护方面，我国仍未出台专门保护个人信息及隐私权的法律，如《个人信息保护法》《个人隐私保护法》等。”〔36〕体系化思维的缺席使得我国信息主体保护的法律呈现出一种“群龙无首”与“杂乱无章”的乱象。

二是缺乏对信息主体利益的实质性保护。在保护的法律手段上，我国多重刑罚与行政追责，而轻民事确权与归责，从而导致在遭受侵权之害时，信息主体的财产与非财产损失得不到或难以得到合理与有效的补偿。

三是对基本范畴缺乏应有的明确法律规定。个人信息是一个与个体的生活安宁、不希望他人侵犯或干涉相关的隐私问题。在隐私权保护上，我国《民法典》已有了历史性的突破，“隐私”一词出现了 14 次，尤其难得的是，《民法典》第 1032 条第一次对隐私定义如下：隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。然而，“私密”的概念循环并没有达到准确无误澄清隐私的效果。同时，“空间”“活动”“信息”都是模棱两可的表述。事实是，何谓“隐私”仍然是一个有权者自由裁量的解释问题。

4. 信息采集标准与共享困境

数据开放与共享是大数据征信的基础，而数据标准化是高效共享的前提。征信数据的标准化建设不仅关系到评价结果的权威性与准确性，而且也益于跨机构、跨行业间的数据资源共享。对于这一问题，自 2005 年起，中国人民银行就启动了征信标准化建设，先后推出了《征信数据元 个人征信数据元》等金融行业标准。此外，为了抑制“以卡养卡”及“拆东墙补西墙”等失信行为，2020 年 1 月中国人民银行征信中心正式启动了第二代征信系统，以填补第一代系统的信息真空。尽管如此，在数据共享与标准化建设方面，我国仍面临以下问题：

一是还没有建立全国统一的信用信息行业标准。实践中，各部门、各行业和地方政府都各自依据自己的判断与利益来建构征信信息系统，从而导致协调性、共享性、效率性差，如“在缺乏统一的信息统筹协调机构下，信息的跨区域、跨系统调配与交流较为混乱”〔37〕。

二是在互联网数据快速增长的当下，各大数据征信机构都根据各自的来源数据、评价模型、统计口径、评级标准等进行信用评估，如此不仅造成同一信息主体在不同大数据征信机构评价结果上的差异性，而且因“数据壁垒所形成的恶性竞争也可能会削弱互联网公司评级结果的公信力”〔38〕。客观上，“存在信息孤岛、数据壁垒未打通、信用信息共享没有畅通渠道是我国当前大

〔35〕 吴双、冯果：《论大数据征信时代下“技法结合”的个人信息保护》，载《科技与法律》2017 年第 4 期，第 42 页。
〔36〕 苏志伟等：《世界主要国家和地区征信体系发展模式与实践》，经济科学出版社 2014 年版，第 24 页。
〔37〕 李真：《P2P 网贷信用征信：金融分析与法律建构》，载《当代经济管理》2015 年第 7 期，第 88 页。
〔38〕 邓舒仁：《关于互联网征信业发展与监管的思考》，载《征信》2015 年第 1 期，第 15 页。

数据征信乃至整个征信行业面临的现实问题”〔39〕。在征信中，大数据征信机构不能获取中国人民银行征信中心的信贷数据，而只能借助关联度较弱的互联网数据来建构信用评价模型。信用数据分割及法律协调的滞后已严重制约了我国社会信用的发展与提质。

（三）小结：破旧立新

“共享经济的不断壮大需要进一步引入信用机制，加快推进信用体系建设，构建以信用为核心的共享经济发展体系。”〔40〕研究表明，“在一个经济体中，如果人与人之间的普遍信任关系越强，那么这样的经济体更倾向于选择市场主导型的金融体系”〔41〕。虽然近年来，我国征信治理的法律制度在不断推进，以中国人民银行为主导的公共征信系统已初具规模，但是在互联网、大数据等技术的催化作用下，信息交换与传递的方式、数据处理、新的征信观念等无不提醒决策者与监管者，世易时移，法律应因时制宜。破茧而出的大数据征信具有一定的“草根性”，其明显的市场性是对政府主导下征信机制的有力制衡与竞争。当社会关系的发展超越于法律之时，法律就处于变革前的十字路口。正视大数据的功效，通过法典的方式对大数据征信进行法律治理的改良就是时代正确与时代必须。

大数据场景与社会信用下，对于我国征信法律治理的走向，以下问题值得深思：需要什么样的理念来引领中国征信的法律治理；如何在宽严相济之间为大数据征信铺设一条成长的康庄大道；信息保护和大数据挖掘之间的角力如何摆脱非此即彼的困境；征信数据如何共享；如何确保信用评价结果的真实性与准确性，从而不偏离预设的社会信用目标……大数据代表了人类文明的进步与自由度的伸展，其既是创新，又是挑战。然而，“文明是诅咒，还是福音呢？在过去，文明既是诅咒，又是福音。至于将来怎么样，则取决于人类是将过去文明中积累起来的知识用于破坏，还是用于建设”〔42〕。

三、社会信用建构的路径：以大数据征信善治为依托

社会信用问题已严重制约了我国的进一步发展，构建一个以“善治”为核心的社会信用评价体系是时代所需所急，因为“善治本身蕴含了主体之间自觉、自愿、自发地达成善，而不是外界强加的治理理想状态”〔43〕。而这也决定了大数据征信必须立足于社会信用这一时代主题。“社会信用治理中，制度、技术与文化三者不可或缺。”〔44〕其中，制度是关键。大数据不单纯意味着人类超算技术的突飞猛进，更昭示着一场法律制度“革命”的到来。如何实现“数据人→诚信人”的转变是大数据时代下征信法律治理必须积极回应的导向问题。

〔39〕 李友元、寇纲：《我国大数据征信的挑战及对策》，载《大数据》2017 年第 1 期，第 31 页。

〔40〕 于凤霞：《完善社会信用体系促进我国共享经济发展的思考与建议》，载《电子政务》2018 年第 8 期，第 81 页。

〔41〕 陈雨露、马勇：《社会信用文化、金融体系结构与金融业组织形式》，载《经济研究》2008 年第 3 期，第 37 页。

〔42〕〔美〕斯塔夫里·阿诺斯：《全球通史：从史前到 21 世纪》，吴象婴译，北京大学出版社 2012 年版，第 195 页。

〔43〕 何哲：《“善治”的复合维度》，载《公共管理与政策评论》2018 年第 5 期，第 46 页。

〔44〕 程民选、李晓红：《社会信用协同治理：制度、技术与文化》，载《华东师范大学学报（哲学社会科学版）》2015 年第 3 期，第 26 页。

（一）法律治理的宏观进路

1. 尊重与敬畏互联网精神

每一种法律制度都是它所处时代的产儿。大数据征信是传统征信的换代，信息共享是征信功能最大化的保障。互联网下的征信大数据“主要涉及传统央行的征信数据、经营数据、身份数据、社交数据、消费/财务数据、日常活动数据、特定场景下的行为数据等”〔45〕。如果法律是从事物的本质出发来寻找其必然关系，那么大数据征信法律治理的进路就必须遵从互联网自由、平等、开放与共享的精神。自由与平等是社会发展的基础。如果我们认同这一观点，那么政府就必须恪守以市场为导向，激励征信机构使用新技术，〔46〕升级其产品与服务，营造良好的技术创新氛围。文明进程中，我们应对市场精神予以足够的肯定与尊重。我们正身处于一个全新的数字时代，经济数字化已对社会信用建构提出了严峻的时代诉求，我国应致力于打造与数字时代相匹配的社会信用体系。

大数据、互联网代表的是这个时代的文明与气息，它不仅是人类科学探索的进步，而且与人类苦求的自由、平等、协作等人文精神不谋而合。这种精神元素无疑是对我国传统中一些根深蒂固的思想、观念，如保守、特权、等级等进行稀释的中和剂。故而，我国大数据征信法律治理改良应以自由、平等、协作、共享精神为导向，从而为其生存与发展留足市场空间，并在具体的规范之间体现中立、客观、公正的社会信用评价功能。同时，以下思想尤为重要：大凡数据，皆可反映信用，借助大数据及云计算等技术手段让数据“保真”与“发声”是大数据征信的根本所在。

“随着移动宽带技术、网络接入技术的迅速提升，更多的传感设备、移动终端能够随时随地接入网络，加之云计算、物联网等技术的带动，中国移动互联网也逐渐步入大数据时代。”〔47〕庞大的用户群体和应用市场使我国成为世界上为数不多的大数据国家，探索大数据征信及其治理，是市场秩序规范、守法守约意识强化、失信惩戒等的重要手段。技术会改造人的思维模式，并决定法律创新的走向，中国大数据征信治理也必须体现与这个时代相得益彰的技术思维，即在互联网、大数据、云计算等技术的支撑下，对市场、企业价值链、整个商业生态圈、治理法律作时代性的考察。

自由是一个规范的概念，在具有利己性的同时，亦具有利他性。如此推演，就是无论产权的归属与所有制形式如何，在大数据征信市场上，任何人都有依其意愿与法定条件决定入市或不入市的权利。法律在其市场准入的态度上应该是，也最好是注册制，而不应该是存在寻租空间的核准制。就平等而言，我们可以从两个层面进行解读：一是不能因入市者身份、产权者等的不同而采取差别待遇，当禁止在立法与监管中进行不公正、不合理的分类时，在大数据征信平等对待的阶梯上，我们就朝前迈进了一大步；二是征信入市与征信业务机会均等。对此，下述观点是发人深省的：“每一个对于一种平等的基本自由之完全适当体制都拥有相同的不可剥夺的权利，而这

〔45〕《互联网征信》课题组：《大数据时代下的互联网征信》，经济科学出版社 2016 年版，第 168 页。

〔46〕技术是一柄双刃剑，如果技术缺乏伦理，那么就如同人缺乏良知。为了消除不确定性，在技术的研发与利用中，必须通过法律的方式对技术设定严格的伦理要求。

〔47〕肖云鹏等：《移动互联网安全技术解析》，科学出版社 2015 年版，第 7 页。

种体制与适于所有人的同样自由体制是相容的。”〔48〕就协作与共享而言，互联网之所以被称为互联网就在于其“相互”与“联接”，其传导的是“团结就是力量”的合作。在市场运转中，竞争从来不是目的，只是更有效合作的手段，对于大数据征信而言，其理亦然。“任何社会在构想和建设社会信用体系时都隐含着对自身社会和文化的预设和理解，不同的社会和文化思维方式影响着社会信用的路径选择。”〔49〕在体现特色时，大数据征信应体现互联网精神。

2. 利益平衡保护

数据是征信业的核心资产，直接影响与决定着行业的命运。大数据给征信业带来的机遇体现在信息源的广阔性、处理的迅捷性、内容的丰富性及征信应景的多样性。然而，“大数据并不是灵丹妙药，作为一种前沿和创新的工具与技术手段，是传统信息技术的延伸和升华，但还不够成熟，还处于尝试阶段。大数据的负面问题——对消费者的隐私侵犯也是不容忽视”〔50〕。在流程上，大数据征信涉及不同的利益，如：在私人利益上，它表现为征信机构的信息采集、使用的商业化利益与信息主体利益之间的对立与紧张；在公共利益上，它关系到征信市场规范、商业秘密与隐私权保护、数据安全及社会信用等公共利益。

社会需要妥协与和平，就必须削弱与杜绝人们之间的相互争斗，将强力法则归属于更权威的规范。大数据征信所涉利益的分切不公直接影响到该行业的发展及社会信用的营造，在监管权、征信权、信息主体权益保护的博弈中，以下思想显得弥足珍贵，即：没有任何一种利益是绝对权利的，也没有任何一种利益是绝对权力的。隐私权保护是大数据征信治理中的前置问题，但是“任何保护隐私的道德义务并不包括限制大数据的义务，因为大数据应用于商业、社会稳定、公共健康和安全感所带来的福利应优于对隐私的关注”〔51〕。

3. 安全原则

互联网开启了一个大数据的信息时代，在这个时代中的人都是数据化的信息人。信息安全与每个社会主体的生存利益密切关联。在丧失强力保护的情形下，人们无异在阳光下“裸奔”。虽然在大数据征信治理的变革中，平等、自由、共享等思想迎合了互联网精神的本质，但是在法律精益求精的设计中，这还并不是价值的全部，它还必须优先考虑安全因素，因为安全是至高无上的法律，安全是利益平衡下大数据其他价值实现不可或缺的基石。

一个公理性的认识是，发展依于安全与秩序，自由与共享等也只有在安全的佑护中才具有真实性，因为“安全有助于使人们享有的生命、财产、平等和自由等其他价值稳定化，并使其尽可能地延续下去”〔52〕。如果大数据征信法律治理的改良是为了实现我中华长久的国泰民安与繁荣富强，那么在我国社会信用建构的开拓进取中，以下思想值得铭记：一个旨在实现正义的法律制度，会致力于在自由、平等、安全等方面创设一种切实可行的综合体，且赋予人的自由、平等和安全应当在最大程度上与人类的共同利益保持一致。

---

〔48〕〔美〕罗尔斯：《作为公平的正义——正义新论》，姚大志译，上海三联书店 2002 年版，第 70 页。

〔49〕黄晓晔：《社会信用建设的逻辑及其路径选择》，载《贵州社会科学》2014 年第 5 期，第 46 页。

〔50〕刘新海：《征信与大数据》，中信出版社 2016 年版，第 7 页。

〔51〕Anita L. Allen, Protecting One's Own Privacy in a Big Data Economy, 130 *Harvard Law Review Forum*, 74 (2016).

〔52〕Christian Bay, *The Structure of Freedom*, Stanford University Press, 1958, p. 19.

4. 体系化思维

体系化是法律科学的必然要求，社会信用治理亦是一项体系性的社会工程。对此，《国家十三五规划纲要》在第 17 篇“加强和创新社会治理”中就专门强调社会信用体系完善，其内容包含健全信用信息管理制度、强化信用信息共建共享、健全守信激励和失信惩戒机制及信用服务市场培育。《信用纲要》的诚信建设就系统地覆盖了政务诚信、商务诚信、社会诚信与司法公信四个方面。就征信而言，“征信体系的建立，有助于识别和监测信用风险、激励借款人按时偿还债务和履约，促进金融和经济发展”〔53〕。社会信用构建是一个政府、市场与社会三方关系理性厘定的系统工程。为了对社会信用体系提供应有的支持，我国大数据征信治理法律的体系化可从以下三个方面进行突破：

一是走法典化的道路，而尽可能地避免走“细则”“暂行”“试行”等解燃眉之急的老路。在这一点，欧盟是比较成功的典范。2018 年 5 月欧盟《一般数据保护条例》（GDPR）正式生效。为回应法律落差与时代需求，该法从管辖范围、数据主体权利强化、数据处理者责任、执法与处罚等方面对前期的规则进行了系统性的革新。法典是通向自由的“圣经”。鉴于当下形散的情况，我国有必要对《征信业管理条例》《征信机构管理办法》及通知类等文件进行归整，使其系统化与整体化。

二是实现辅助性法律对征信治理体系化的外部支撑。独木难成林，体系内的征信治理法律的有效运转、市场规范与利益平衡等还需要体系外的制度扶持，从而形成一个良好的内外循环系统。在该问题上，美国的做法是值得借鉴的，如除了《公平信用报告法》，其还专门配备了《公平债务催收法》《金融隐私法》等多部法律，形成了一个完整的征信法律体系。

三是建立体系性的社会信用。根据《信用纲要》等文件的精神，构建一种系统的社会信用体系是国家治理的目标。“由于我国建立的是广义的社会信用体系，因此还需要围绕公共信用信息管理、信用监管、红黑名单管理、联合奖惩等方面建立有中国特色的信用立法。”〔54〕政府信用、企业信用与个人信用是社会信用体系三大鼎立的支柱，而在这之中，政府守信是重中之重，为法治政府的要义所在。在大数据征信治理中，有必要对征信对象作扩张性规定或解释，征信对象不仅应包括自然人、营利法人，同时也应包括社会团体、事业单位、社会服务机构、基金会等非营利性法人及特别法人，以最大可能地让大数据征信覆盖社会中的每一个角落，而无论其是权利者，还是权力者。

（二）微观关键性问题的应对之策

1. 大数据征信准入条件

当下，一些无牌照、无约束甚至非法的机构和个人正在通过各种途径采集、倒买倒卖公众信息，以牟取暴利，从而对正规征信机构产生劣币驱良币的逆淘汰效应。因此，严格规范大数据征信平台的市场准入标准是当务之急。虽然对于入市条件，《征信业管理条例》《征信机构管理办法》等从股东信誉、最低注册资本金、任职资格、信息系统安全等方面作了硬性要求，但是大数

〔53〕 郭熙保、徐淑芳：《全球征信体系的制度安排及其影响因素》，载《学术研究》2005 年第 11 期，第 31 页。

〔54〕 韩家平：《关于加强社会信用立法的思考与建议》，载《征信》2019 年第 5 期，第 5 页。

据与互联网语境下，仍有必要对入市条件作更细致的推敲，以应对技术的要求。大数据意味着，“新的信用风险体系的一个颠覆性的基本思想是一切数据皆信用，这需要大数据技术来支撑”〔55〕。是故，除了注册资本等常规性的准入条件外，对拟新设的大数据征信机构与业务拟大数据化的原征信机构更应注重信息安全保障的软硬件设施、数据处理能力及内部控制等审慎要求。2017 年 6 月开始实施的《网络安全法》涉及网络运行安全、信息安全、监测预警与应急处置等重大内容，它标志着网络空间必须依法而治，这也为我国大数据征信机构的软硬件配置标明了底线条件。数据是大数据征信的基石，除了一般要求外，还必须通过法律明确大数据生命周期安全的概念，强调“大数据生命周期的安全以数据为中心，重点考虑大数据生命周期各环节中的数据安全问题”〔56〕。

由于个人数据直接涉及隐私权，且在财产数据化的时下，个人数据关系到公民的财产安全，所以对经营个人征信业务的征信机构的信息安全保障标准应高于经营企业征信业务的标准。虽然个人征信与企业征信存在一些差异，如企业征信市场发展自主性强，不涉及隐私权保护，但是当这两种业务混同于同一机构时，应将风险隔离墙作为入市的重要标准。如此，不仅可以防止信息泄露风险在同一机构不同部门之间传递，而且也可以作为一种未来可能涉诉案件的防御性抗辩。在具体要求上，征信机构应采取物理空间隔离、人事独立、财务分置、网络系统分离、业务分开等方式构筑个人与企业征信业务风险交叉传染的防火墙。

2. 大数据征信规则的优化

虽然《征信业管理条例》对信息采集范围、采集程序与方式、负面信息保留期限等进行了规定，但只是确定了基本原则，专业性与操作性不强。针对这种现象，可从以下几个方面进行精进：

一是进一步明确数据采集与加工的合法边界。采集的合法性不仅关系到大数据征信机构数据产品商业化目的之实现，而且也可以保证各主体之间的利益平衡。在这一点上，我国《个人信息保护法（草案）》已有了实质性的突破，如该文件将个人信息界定为：以电子或其他方式记录的与已识别的自然人有关的各种信息，不包括匿名化处理后的信息。个人信息处理应采用合法、正当的方式，并遵守公开、透明与诚实信用原则。同时，文件在明确个人敏感信息的基础上，确立了强力保护的规则，如必须取得信息主体的同意，并事前告知可能的影响等。

二是确保征信信息的准确性。征信数据质量不仅事关信用状况的公正评价，而且也关系到征信社会信用功能的实现，如美国 1996 年的《消费者信用报告改革法》就强调，征信机构必须对消费者投诉的不准确信息进行查实，将核查结果告知消费者，且必须通过全国征信机构的联合通知系统将该结果向其他征信机构公开。若经调查，信息失实，则必须在 30 天内予以删除，且不得重新写入。

三是强化信息主体的制衡作用。信息主体的异议权与投诉权不仅益于信息的准确性，而且也能督促大数据征信机构在信息采集与加工中尽到谨慎与勤勉的义务。社会信用建构中，“阳光”

〔55〕 刘新海、丁伟：《大数据征信应用与启示——以美国互联网金融公司 ZestFinance 为例》，载《清华金融评论》2014 年第 10 期，第 98 页。

〔56〕 陈兴蜀等：《大数据安全保护技术》，载《四川大学学报（工程科学版）》2017 年第 5 期，第 4 页。

是失信行为最好的消毒剂。为了保证信用评价的客观性，应强化征信机构免费为信息主体提供其个人信用报告的义务。

为了不让这一目的落空，有必要对信息主体的诉讼救济作以下安排：当信息主体对征信机构的异议权不能实现时，其可以通过民事诉讼的方式来维护其权益。同时，在证据规则上，可考虑实行举证责任倒置。“如果要求消费者来证明信用报告机构存有过错，这将置其于不利地位，因为后者很可能占有所有信息。在诉讼中，信用报告机构占有绝对的资源优势，且实际损害极难证明。”〔57〕征信的目的在于失信惩戒，但是“信用联动奖惩机制设计的初衷并不是要一棒子将失信者彻底打死，而是要让失信主体付出代价后，知晓守信的重要性，给予失信主体改过的机会”〔58〕。因此，在大数据征信治理中，本着社会信用的目标，应允许失信人在法定条件下享有信用修复与补救的权利。

3. 隐私权保护强化

大数据时代，由于个人信息的获取、存储、传播等所涉环节错综复杂，由此形成了一条盘根错节的黑色利益链。App 泛滥之下，对个人信息的过度开发与采集使公民的隐私面临前所未有的危机。客观上，“只有遵守保护个人信用信息隐私权的一系列原则，征信活动才能在正当范围内进行”〔59〕。因此，在大数据征信法律治理的解构中，对该隐私权保护的程度与有效性直接影响到征信制度的正义。虽然《征信业管理条例》用排除法圈定了信息的可采集区域，但这是否就意味着，凡不在排除范围内的信息，均可自由采集呢？在公民因信息外泄而不堪其扰时，这是一个必须认真对待、兼有法律性与政治性的复合性问题。实质上，强力保护网络用户的个人隐私与大数据征信是两个并行不悖的问题。对个人隐私的有效保护能使网络用户无后顾之忧地使用网络，从而通过消费等促进互联网及大数据征信的发展。大数据征信蕴藏着巨大的公共利益与秩序，隐私代表着私人空间与权利。大数据下，如果法律不能在公域与私域之间做到泾渭分明，那么隐私权保护的前景也并不乐观，因为“在政策是否有必要调整上，我们过去的探讨多集中于原则，但是现在我们的讨论越来越务实，比较关注保护的成本”〔60〕。

大数据技术加剧了隐私的“电光化”风险，这也促使我们不得不在新形势下对隐私权作出时代性的解读。时下，如果我们对隐私权的认知仍停留于传统的“个人安宁的生活不受干扰”的消极权利，那么这显然背离了互联网、云计算等社会技术背景。实际上，大数据催生了个人信息隐私权走向何方的时代命题。虽然我们可通过单行的规则来应对这一问题，如将向他人出售、提供公民个人信息情节严重的行为入罪，但是相对于个人信息的系统保护而言，这只是“杯水车薪”。如果我们治理的目标是致力于构造厚实的个人信息保护的“法律长城”，防止征信机构等权利/权力的滥用，那么就有必要出台专门性的“个人信息保护法”，并重点考虑以下几个问题：

---

〔57〕 Austin H. Krist, Large-scale Enforcement of the Fair Credit Reporting Act and the Role of State Attorneys General, 115 *Columbia Law Review*, 2319－2322 (2015).

〔58〕 肖卫兵：《我国社会信用立法若干问题探析》，载《电子政务》2017 年第 6 期，第 68 页。

〔59〕 张晓军：《论征信活动中保护个人信用信息隐私权之目的特定原则》，载《中国人民大学学报》2006 年第 5 期，第 86 页。

〔60〕 Gus Hosein, Returning to A Principled Basis for Data Protection, 84 *Chicago-Kent Law Review*, 803－809 (2010).

一是与时俱进地明确隐私权的内容。虽然对隐私权进行抽象的概括能起到指引的效果，但是为了消除“市场假象”，还必须对隐私进行详细的列举。数据隐私时代，增强数据主体权利是对抗不法侵害最有力的武器。欧盟的 GDPR 就体现了这一思想，如该法专门确立了数据主体的更正权、删除权、限制处理权与携带权。

二是将“从设计着手保护隐私权”的思想植入到软件产品研发与销售的管理中。“在电子化时代，数据保护面临诸多挑战，为了强化对个人隐私权与数据的保护，在新的法律框架中应要求相关企业将保护隐私权的概念融入其产品设计中，而不是完全依赖于那些没有多少人愿意读的隐私保护政策。”〔61〕同时，可考虑将隐私权保护纳入大数据征信机构的日常合规管理，“公司应该持续地对其数据采集、储存、分析与使用的政策进行评查”〔62〕。

三是可考虑根据信息的敏感度不同，确立强弱相宜的保护标准。虽然我国《个人信息保护法（草案）》已体现了这一精神，但是这些纲领性的规定更多只是指明了保护的方向，难以满足现实的保护诉求。为了解决这一困境，有必要采取列举的方式对一般类和敏感类数据进行说明，如敏感性数据包括种族、宗教信仰、政治倾向、健康状况、世界观等。对敏感类数据，根据侵害程度、情节等的不同，分层级性地给予严格的保护，并规定除法定例外情形外，不得对敏感数据进行处理。

四是严格控制与规范金融、征信、电信、交通、教育、医疗等大众型服务机构对消费者的信息保密义务。同时，对政府部门利用公权力泄露个人信息的行为进行重点遏制。在个人信息采集上，确立有序开放原则，即“个人信用信息的开放、收集、加工、披露和使用，都应制定并遵守一定的法律规则，力戒个人信息无序开放和随意滥用现象的发生”〔63〕。

4. 征信信息共享机制的建构

“征信的本质是实现信息分享，全面反映信息主体的信用状况”〔64〕，从而降低当事人的逆向选择风险，防范可能的道德风险，并对风险进行准确定价。“在我国，政府主导下的征信体系建设取得了显著的进步，但是征信体系建设的目标并非一个完全由政府控制的公共征信体系，而应是一个高效的面对市场的征信体系。”〔65〕市场是一个比较优势理论下，开放、共享、协作的概念。由于体制的原因，目前大量的信用信息分散存留于工商、税务、法院、公安等部门或政府搭建的信用数据系统。“走向成熟的社会主义市场经济途中的当代中国，必须把信用与诚信意识作为一种经济、政治、文化的准则，全面融入社会生活中。”〔66〕大数据下的社会信用建构急需破除“数据孤岛”，坚持中立的第三方信用评价，注重市场机制效应，从而体现信用社会治理的公开、公平与公正。

对于数据共享，我们可以采取分步走的方式：一是在整合的基础上，推进政府各部门的信息数据与金融信用数据库的“紧密对接”，从而加快跨部门、跨区域的信用数据资源的共享、开发

〔61〕 Rebecca Wong，Data Protection：The Future of Privacy，27 *Computer Law & Security Review* ，53－57（2011）.
〔62〕 Hugh J. Watson，Addressing the Privacy Issues of Big Data，19 *Business Intelligence Journal*，6（2014）.
〔63〕 吴国平：《个人信息开放与隐私权保护》，载《法学杂志》2005 年第 3 期，第 75 页。
〔64〕 王晓明：《征信体系构建制度选择与发展路径》，中国金融出版社 2015 年版，第 10 页。
〔65〕 李清池等：《信用征信法律框架研究》，经济日报出版社 2008 年版，第 102 页。
〔66〕 俞思念：《对我国社会信用体系建设的再思考》，载《湖北社会科学》2018 年第 1 期，第 26 页。

与利用。二是指引、鼓励不同类别的征信机构之间的信用数据共享。为了打破自我循环，我国应尽可能地统一线上与线下的征信标准，统一接口规范，确立平台、机构之间数据资源互通有无的指导性规则。同时，由于征信的目的在于信用风险识别，所以在征信大数据应用时，不能奉行“全部拿来主义”，而应剔除一些无关联或关联度不大的数据，只筛选房租缴纳、遵纪守法、话费交付、公共事业缴费、支付交易、信贷记录、学术诚信等关键数据，并以此作为共享的基础。三是鼓励大数据征信平台数据库系统的建设。若大数据征信系统与金融信用基础库之间存在映射关系，则可以考虑将其收纳为中国人民银行征信系统的子系统。四是有条件地尝试将成熟的大数据征信企业接入中国人民银行的征信系统，从而实现数据资源的共享与共建。

征信数据资源共享是一个与征信标准化建设相关的问题。当下，我国在征信标准化方面还远没有实现数据接口、信息分类及资料定义等基础技术标准的统一。为了打破这一僵局，我国可以考虑由中国人民银行牵头制定全国统一的信用信息采集与分类标准、信息主体标识与基本术语规范及接口标准等，并根据大数据征信的特点，对相关标准进行针对性的改造，以保证其标准性、科学性与效率性。同时，鼓励龙头性的大数据征信平台根据自身的行业要求研发征信标准，在经过认证与评估后，可考虑将其升级为国家行业标准。

5. 法律责任完善

制度不可能建立在无私的爱与宽容之上。为了权威、尊严及宣告法律的激励或惩罚信用，法律必须有牙齿。虽然我国《征信业管理条例》等用专章规定了征信机构不作为的法律后果，但是其存在责任主体覆盖范围狭小与民事责任虚置等缺点。而且，“征信机构与被征信的消费者个人权利义务存在严重的不对等”〔67〕。若大数据征信机构意图与政府携手在信用中国打造中扮演一个不可替代的角色，那么依法依规征信，并保证信用评价的公正性就是其职责所在。为了确保处于强势地位的大数据征信机构在运营中不偏离预设的社会信用与信用国家目标，就必须增加其违规的成本。为此，我国可以已设定的“法律责任”为基础，构建一个“民事→行政→刑事”由弱渐强的法律惩罚信用责任体系。

服务于社会信用治理是大数据征信机构存在的理由，但其又是市场的，为了生存与逐利，基于利润最大化，在征信中，其可能存在角色滥用风险，且大数据的运作模式更是放大了这种风险。是故，一个基本的逻辑是，为了对征信机构可能的失信行为进行惩戒，其责任与苛刻程度应大于其他社会主体的失信行为。在该问题上，可从以下三个层面进行规划：一是私益保护方面。作为链接存在的网络化数据是大数据征信的基础，为了保护公民隐私权、企业商业秘密及保证信用评价的客观性等，必须加大征信机构失信的民事赔偿责任。二是公益保护方面。征信具有高度的公共利益性，若大数据征信机构的所作所为违背了这一宗旨，那么就必须快速高效地进行高强度的行政责任问责。对涉嫌犯罪者，则雷霆式地依法追究当事人应承担的刑事责任。三是法律责任形式均衡问题。在责任承担中，应避免重行政责任而轻民事责任，或以刑代民的倾向。虽然行政与刑事责任能让失信的征信机构与直接责任人有“切肤之痛”，但这并不是“雪藏”民事责任的理由。为了让私益与公益都能得到平等的保护，在实践中，必须避免以行政或刑事责任替代民事责任的误区。

〔67〕 李晓安：《我国社会信用法律体系结构缺陷及演进路径》，载《法学》2012 年第 3 期，第 150 页。

四、结语：一个以社会信用为本位的主题

“信用制度建设的目的不是单靠严厉的外控，更在于通过长期的约束机制最终使人们将外在的行为约束变成一种行为习惯，让诚信和信任再度恢复。”〔68〕毋庸置疑，服务于长效性的社会信用是大数据征信的时代性主题。大数据征信是一个与创新相关的命题。创新即创造性的破坏，它意味着旧观念、旧秩序与旧制度的消融、解体，及新思维、新秩序、新制度的萌芽与解构。大数据是现代征信模式的标签，“在宏观上，大数据是认识论的变革，大量对象从不可知到可知，从不确定性到精确预测，从小样本近似到全样本把握，是认识世界和改造世界能力的升华”〔69〕。这种成长的力量也使得传统的征信与治理面临一场迫在眉睫的“变革”或“被变革”。变革中，我们应先盯住的是社会信用与人类命运共同体的宏大目标，而后才是我们究竟需要什么样的法律。

在倡导兼容并包精神的社会中，如果殚精竭虑地试图从法律是什么的角度来实现社会成员之间友爱共处共存的目标，还是远远不够的，因为除了稳定与安全，现实的法还应服从于正义性目标。社会信用的确立、维护与矫正需要私人与国家之间的紧密协作。然而，问题是如何恰到好处地把握国家权力介入的程度。在强烈体现国家强力意志的法律创新中，适度引入自然法的理念无疑能够对我国大数据征信的法律治理起到警惕与监督作用，因为“自然法的重要性也许不在于解决一个文明制度中出现的正常问题，而在于它有助于决定什么才是一个文明的法律制度”〔70〕。此外，在新的事物还没有最终尘埃落定之前，尊重市场优胜劣汰的自然法则，给予一定的发展空间，保有适度的耐性与宽容也是非常必要的。

Abstract：Social credit is the basis for the maintenance of social order，harmony of interpersonal relation，normalization and development of transaction，people's richness and prosperity of the nation，which is of great significance for construction of destiny community. The big data is changing the mode，way and idea of traditional credit investigation and produces the evolutionary effect on the renewal of the governance of credit investigation. Big data investigation promotes the construction of social credit and the formation of credit nation. As the modifier of social interests and stabilizer of social order，when the crediting regulatory law obviously lags and creates contradiction between supply and demand，it is a reasonable selection to initiate the innovation from social credit，specified idea，balanced protection of interests，market safety and respect of the nature of internet.

Key Words：social credit，big data credit investigation，credit china

（责任编辑：刘权　赵建蕊）

〔68〕 黄晓晔：《信用与社会控制——解读社会信用危机的新视角》，载《学术研究》2013 年第 12 期，第 79 页。
〔69〕 王达：《美国互联网金融与大数据监管研究》，中国金融出版社 2016 年版，第 182 页。
〔70〕〔美〕波斯纳：《法理学问题》，苏力译，中国政法大学出版社 2002 年版，第 303 页。

财经法学 No. 4，2021
pp. 41 - 51

论流量传导行为对数字经济平台市场力量的影响

杨　东　王　睿*

内容提要：流量传导行为不等同于数据的传输或集聚，其具有独立于数据而被单独讨论的意义。鉴于平台导流行为的表现形式因平台商业模式的不同而有所区别，故应对该行为分场景予以分析。从宏观层面来看，导流行为使杠杆效应更易实现，并且提高了市场的进入壁垒。根据这些效果，可以认定导流行为有增强平台市场力量的作用。从这一效果的具体实现路径来看，流量传导行为对平台的直接影响是带来流量即用户注意力，精确匹配的算法又极大地提高了流量价值的转化率，加强了流量利用的确定性。而且，流量传导的过程同时也是数据积累的过程，其通过提高平台数据的更新速度，助力平台将流量优势转化为数据优势，加剧数字经济平台领域的“赢者通吃”现象。

关键词：流量传导行为　平台　市场力量　垄断

数据作为一种新型生产要素，已经进入了法律规范的视野。《中华人民共和国反垄断法》（以下简称《反垄断法》）修订草案在“滥用市场支配地位”一章中，将“掌握和处理相关数据的能力”作为认定平台经营者具有市场支配地位的考量因素。但是，对静态数据的关注不足以完整展现数字经济平台市场竞争的逻辑和全貌。考虑到平台商业模式需要以流量为依托，且流量与数据之间具有紧密联系并相互作用，数据价值实现的各环节离不开流量的传导。因此，对动态的流量传导，以及促成流量传导的经营者行为更应予以重视。

在工业经济时代，流量被用来描述线下商铺的人流量。人流量大意味着有更多的人光顾商家，商家卖出商品、获取盈利的可能性也就越大。在数字经济时代，流量从线下转移到线上，被

* 杨东，中国人民大学法学院未来法治研究院教授，中国人民大学民商事法律科学研究中心研究员；王睿，中国人民大学法学院硕士研究生。

本文为国家社科基金重大项目“在法治轨道上促进平台经济、共享经济健康发展研究”（21ZDA025）的阶段性成果。

赋予新的内涵。有学者指出，流量是用来描述访问一个网站用户数量以及用户所浏览页面数量等的相关数据指标。〔1〕还有学者就这些指标进行了罗列，认为其包括独立访问量、重复访问量、页面浏览数、每个访问者的页面浏览数等。〔2〕

数字经济平台获取用户流量的方式可分为两种，一种是通过产品研发、宣传推广等方式吸引用户参与或使用，实现流量的“从无到有”。这一方式往往为初创企业使用，需要时间进行流量积累，对平台市场力量的影响见效较慢。另一种则是通过流量传导，直接、快速获取大量用户的注意力。鉴于数字经济平台对流量的高需求、强依赖，流量传导无疑会对接受传导的平台产生正向反馈，深入影响平台的市场力量。

流量传导现象并非总是自然而然地发生，其背后往往存在平台经营者有意的行为。实际上，能够加快流量传导速度、操控流量传导方向的流量传导行为已被普遍应用于同一平台生态之中，或不同平台生态之间。流量传导行为常被看作是平台企业的自主商业策略或宣传手段，而被法律规范所忽视。但在数据竞争加剧竞争动态性、跨多边市场竞争和未来竞争要求规制链条前移的背景下，〔3〕流量传导行为在《反垄断法》语境下的意义值得特别审视。探究流量传导行为对数字经济平台市场力量的影响，有助于把握平台的发展趋势和市场力量的延伸方向，评估导流行为的反竞争效果，从而为规制提供理论基础。

一、流量传导行为的场景及传导效果

数字经济平台基于公域流量掌握着流量入口，并倾向于利用流量控制权增强市场力量。流量传导行为就是平台行使流量控制权的一种重要表现形式。流量传导的效果可以通过两种方式实现：其一，平台通过流量在自身生态间的传导，利用杠杆效应推动平台市场势力的快速扩张；其二，平台通过流量传导行为可以制造“流量池”，直接提高市场的进入壁垒，限制潜在竞争对手的发展。

（一）流量传导行为的场景分析

流量可以承载数字经济平台的商业运营模式，互联网平台的经营实际上就是建立在庞大流量上的经济行为。不同场景中的流量种类和利用方式有所不同，而平台和场景并非处于一一对应的关系。这意味着，尽管是同一平台上的流量，也不能一概放在同一场景中看待，如微信广告的流量合作生态就是由朋友圈流量与公众号、小程序、小游戏的流量共同构成。〔4〕同样的，流量传导行为也应该被置于场景下进行分析。

需要先行明确的是，流量传导行为作为一种推广措施，可以由任何互联网企业甚至个人实施。但受实施主体不同、产品或服务对用户的吸引力高低不同等因素影响，流量传导的效果会有所区别。鉴于数字经济平台掌握着流量入口，其实施流量传导行为的效果更为显著，导流行为对

〔1〕 参见季境：《互联网新型财产利益形态的法律建构——以流量确权规则的提出为视角》，载《法律科学》2016 年第 3 期。
〔2〕 参见马晓明、翟静芳：《网络不正当竞争损害赔偿研究——以流量、数据为视角》，载《电子知识产权》2019 年第 12 期。
〔3〕 参见陈兵：《因应超级平台对反垄断法规制的挑战》，载《法学》2020 年第 2 期。
〔4〕 参见《微信广告首次对外公布流量数据：月入 10 万以上的流量主超过 600 个》，载《城市党报研究》2019 年第 2 期。

市场力量造成的影响更易观察，故接下来关于流量传导行为的论述，都是围绕“数字经济平台”作为该行为的实施者这一前提展开。

流量传导行为并不等同于数据的传输或集聚，其表现形式是多样化的。流量传导行为可能发生在同一个平台生态中，即平台为自己的不同服务类别提供流量传导路径，以拓展业务范围。如微信在其平台上为短视频、移动支付等功能提供了跳转的接口，用户通过点击“视频号”“支付”可以进行跳转，此时就实现了移动社交领域的用户流量向短视频、移动支付等市场的传导。

流量传导行为也可能发生在不同的平台生态之间，即平台为那些向自己支付流量对价的主体提供导流服务。如微信的“朋友圈”和 QQ 的“动态”中时常出现的嵌入式广告，就展现了腾讯的流量传导行为。这些广告会展示相关商品或活动的图片、视频，并搭配文字表述，提供跳转链接。微信和 QQ 的用户一旦打开朋友圈或 QQ 动态，就有机会看到这些广告，并可能被广告吸引而点击相关链接，跳转到广告主提供的页面上，或者直接进入另一个应用，由此实现腾讯用户流量向广告主的导入。

总而言之，流量传导行为具有多样态的特征：既可能是单向的，也可能是双向的；既可能是有偿的，也可能是无偿的；实施主体可能是单方的，如平台企业为自己旗下的新产品导流，也可能是双方或者多方的，如平台向与其达成合作协议的主体导流。

（二）导流行为使杠杆效应更易实现

在数字经济中，市场与市场之间的边界变得不再清晰，超级巨头跨界实施控制的成本很低。再加上网络效应在互联网行业常表现出正反馈，大型网络对用户更具有吸引力，并倾向于变得更大。〔5〕因此，数字经济平台大多具有向其他市场传导力量的倾向。

流量传导行为是数字经济平台常用的一种传递市场力量的方式。流量本身就具有可流动性，其能够在各个平台间、平台的各板块间流通，并因此成为平台多元业务协同的纽带。平台借助导流行为，可以将现有的优势传导到通讯、社交、阅读、支付、购物、交通出行等其他市场，〔6〕从而实现垄断的自我强化。如腾讯的核心领地虽在社交、游戏、第三方支付方面，但也在不断向短视频、云计算等领域进攻。字节跳动在短视频、秀场直播、信息流媒体方面占据优势地位，但也没有放弃向传统电商、O2O 电商、教育、游戏等领域的发展。各互联网巨头都倾向于多条战线“作战”，希望能够通过发展多元自有业务提升流量变现的效率。有学者将这一过程概括为“平台通过增强及扩张服务，进入新的领域，将在新的领域形成第二轮垄断、第三轮垄断”〔7〕。

数字经济平台利用其在一个市场上的垄断力量来获得在另一个市场上的垄断力量，从而同时控制两个市场的现象，可以用“杠杆效应”来描述。传统理论通常认为搭售、捆绑销售、独家交易等行为具有杠杆效应，但在数字经济时代，杠杆效应的内涵已经发生了变化。一方面，在垄断力量的衡量上，应将平台的用户数量和活跃度，以及平台获取数据的能力纳入考虑。因为控制着流量入口的数字经济平台，往往更有能力利用综合优势向其他市场渗透，通过“杠杆”形成在新

〔5〕 参见张素伦：《互联网背景下反垄断法实施理念研究》，载《河南师范大学学报（哲学社会科学版）》2016 年第 4 期。
〔6〕 参见杨东：《警惕数字平台“赢家通吃”》，载《人民政协报》2020 年 11 月 26 日，第 7 版。
〔7〕 参见李勇坚：《互联网平台寡头垄断：根源、影响及对策》，载《人民论坛》2021 年第 Z1 期，第 14 页。

市场领域的竞争优势。〔8〕另一方面，互联网平台滥用杠杆优势的行为外观与搭售、限制交易等排他性行为存在根本差异。在“可口可乐并购汇源案”中，执法机关认为若允许并购，可口可乐公司将有能力把其在碳酸饮料市场上的支配地位传导到果汁市场，削弱、剥夺其他果汁生产商与其竞争的能力，使消费者被迫接受更高价格、更少种类的产品。〔9〕可见，传统说理更强调对搭售“强制性”的论证。但具有免费模式、动态竞争等特点的平台经济显然难以适用这一论证思路。〔10〕

互联网平台不需要通过强制手段传导市场力量，平台的流量传导行为足以使杠杆效应更容易实现，且这种市场力量传导的方式具有非强制性和隐蔽性。有学者提出，在平台经营模式下，互联网企业的竞争在平台接口层面、应用层面分别或者综合地展开。〔11〕这意味着，互联网平台不需要通过强制手段要求其他经营者、消费者接受搭售的产品或者与其独家交易。平台只要能够把握端口，也就是控制流量的传导，就可以直接实现市场力量的传递。如 2017 年 6 月，谷歌因滥用支配地位操纵搜索结果，不公平地把客户引向自己的购物服务，被欧盟处以 24.2 亿欧元的罚款。2020 年 12 月，谷歌因通过实施“搜索歧视”将自有资源的搜索结果置顶，被美国 38 位州和地区总检察长组成联盟提起诉讼。〔12〕在这两起案例中，谷歌都试图通过其在搜索引擎市场的支配地位，用非强制性的手段获取在购物服务等其他领域的市场力量，佐证了流量传导的非强制性使杠杆效应更易实现的观点。

（三）导流行为提高了市场进入壁垒

有学者提出，测算市场力量的潜在思路是，评估在位者因忌惮新进入者而在商业行为方面制造障碍的程度，〔13〕即观察市场中的现有竞争者通过实施某些商业行为，能否有效提高市场的进入壁垒。有学者提出了“数据池”的概念，认为“数据池”的组成成员不愿对外共享池中的数据，从而为反竞争协作的达成提供了条件。〔14〕虽然流量传导行为不同于“数据池”的组建，但是特定范围内的流量传导可以被看作在这一范围内划定了“流量池”，同样具有将流量传导范围外的经营者置于竞争劣势地位的作用。

流量传导行为正是这样一种制造“流量池”以提高市场进入壁垒的商业行为。具体而言，流量传导行为可以使流量通过两种方式成为市场进入壁垒。一方面，流量可以作为数据的来源和基础，间接构成市场进入壁垒。另一方面，流量也可以作为平台“获取数据的能力”的表征，单独、直接构成市场的进入壁垒。

前者的逻辑在于，流量可以为平台带来用户，用户在使用平台时则会留存数据。因此，流量

〔8〕 参见前引〔7〕，李勇坚文。

〔9〕 参见邓峰：《传导、杠杆与中国反垄断法的定位——以可口可乐并购汇源反垄断法审查案为例》，载《中国法学》2011 年第 1 期。

〔10〕 参见叶明、黎业明：《互联网平台滥用杠杆优势行为的反垄断规制研究》，载《管理学刊》2021 年第 2 期。

〔11〕 参见张江莉：《互联网平台竞争与反垄断规制：以 3Q 反垄断诉讼为视角》，载《中外法学》2015 年第 1 期。

〔12〕 参见王先林、方翔：《平台经济领域反垄断的趋势、挑战与应对》，载《山东大学学报（哲学社会科学版）》2021 年第 2 期。

〔13〕 参见王璐、方燕：《互联网领域垄断行为界定与市场力量测度》，载《中国流通经济》2021 年第 2 期。

〔14〕 参见时建中、王煜婷：《“数据池”共享行为的竞争风险及反垄断法分析》，载《江淮论坛》2021 年第 2 期。

可以被看作是基于用户使用行为而形成的一系列数据集合。又由于数据具有一定程度的排他性、质量和价值的差异性、高昂的收集成本、锁定效应和转换成本以及网络效应等属性，故其会提高数据市场的进入壁垒。〔15〕但数据作为市场壁垒的观点也遭到了一些质疑。有观点认为，数据的时效性可能使数据掌握者的优势地位被削弱，且企业的竞争劣势受到算法技术、产品质量、经营策略等多方面因素的影响，数据持有量本身不足以构成市场壁垒。〔16〕

流量作为数据来源，间接构成市场进入壁垒的观点，因学界对“数据”作为市场壁垒的质疑而受到了一定冲击。但这些质疑反而证实了动态的流量与静态的数据量相比，更可能帮助平台形成竞争优势，也即流量能够脱离数据而单独构成市场壁垒。平台的建立和发展往往需要以大量流量为依托，其商业模式能否成功实现，与流量的获取速度和质量密切相关。若流量已经被集中于少部分企业，重新获取流量难度较大或所需时间过长，则新进入的企业无疑会面临现实阻碍。换言之，当代表“获取数据的能力”的流量被作为平台从事市场竞争的前提条件，而市场新进入者又无法收集类似数据或购买访问权限时，现有企业拥有的访问数据的权限就构成了一种市场进入的障碍。〔17〕

当前，执法机关也已经关注到了数字经济时代存在特殊的市场壁垒。2021 年 4 月 10 日，国家市场监督管理总局对阿里作出的《行政处罚决定书》提到，“网络零售平台在平台一边获得足够多的用户”是实现“有效市场进入”的关键。鉴于“用户数量”是可以衡量“流量”大小的因素，可以认为《行政处罚决定书》的这一表述佐证了流量单独构成市场进入壁垒的观点。

二、流量传导行为影响平台市场力量的具体路径

平台的流量传导行为使杠杆效应更易实现，且会提高市场的进入壁垒。这两种效果的叠加无疑增强了实施导流行为的平台的市场力量。但是，就“流量传导行为”和“市场力量”之间关系的观察，不应仅停留在对导流效果的宏观分析层面。流量传导行为增强平台市场力量的具体路径需要进一步阐释，特别是流量传导行为与用户注意力之间的关系、算法对流量利用率的提高作用、流量优势向数据优势的转化等问题。

（一）导流行为带来用户注意力

正如前文所述，流量可以用用户数、浏览量等数值衡量，而这些数值又能够被用来描述用户注意力或关注度的多少。因此可以认为，流量与用户注意力的内涵相近，流量是用户注意力的具象化。注意力是当今越来越重要的一种资源，互联网经济的本质就是注意力经济。依赖于注意力市场的注意力经济商业模式是目前许多社交、科技平台的主要商业模式。但用户注意力的总体规模是有限的。有学者曾提出，互联网的人数乘以平均上网时长，就是国民线上总时间。由于所有网上消费都在这个时段内进行，因此可以认为，这相当于互联网消费市场规模的边界。〔18〕

〔15〕 参见殷继国：《大数据市场反垄断规制的理论逻辑与基本路径》，载《政治与法律》2019 年第 10 期。
〔16〕 参见陈兵：《“数据垄断”：从表象到本相》，载《社会科学辑刊》2021 年第 2 期。
〔17〕 参见任超：《大数据反垄断法干预的理论证成与路径选择》，载《现代经济探讨》2020 年第 4 期。
〔18〕 参见《数字经济，解构与链接——人文清华讲坛江小涓演讲实录》，载微信公众号“人文清华讲坛”，2020 年 11 月 22 日。

在用户注意力有限而互联网企业众多的情况下，抢占注意力无疑成为各互联网企业的重点策略。流量传导行为就是互联网企业抢占用户注意力的一种表现形式。有学者将注意力经纪概括为：注意力经纪人通过向公众提供新闻、娱乐、免费服务以吸引其注意力，再将注意力转卖给广告商以获取现金收益。〔19〕这一商业模式就是一种有偿的流量传导行为。其特点在于，接受流量传导的主体如广告商，不需要第一时间直接接触用户群体，而由直接面对用户群体的注意力经纪人如数字经济平台，负责通过提供免费服务等方式吸引用户。之后由注意力经纪人通过流量传导行为为广告商提供推广，并从广告商处获取报酬。除这种有偿获取流量传导的方式外，互联网企业也可以选择不通过注意力经纪人，而凭借自身发布的广告、补贴等方式，向其潜在的或现有的用户推送新产品、新服务。但这一模式在该互联网企业本身就具有一定的用户基础，也即建立起自己的流量生态时，才能起到较好的流量传导效果，实现新产品和新服务的推广。

对平台而言，流量传导行为的最大意义在于其能够带来用户的注意力，为自己或与其达成合作的广告商提供更多的交易可能性。从这个角度来看，流量也可以被理解为交易的机会。交易机会正是互联网经营主体争夺的对象，也是经营主体能够量化的价值体现。〔20〕当然，流量传导行为的最终效果仍取决于用户的兴趣和接受度。用户是否同意接受推送、是否对推送内容感兴趣并愿意点开链接，决定着流量传导的效果如何。因此，从某种程度上来说，流量传导行为只是给被传导者提供了一个“被展现给用户的机会”，而不必然给被传导者带来有黏性的用户。当然，不成功的流量传导也并非没有讨论意义。实际上，在关注“行为”的我国反垄断法的分析框架中，可能带来用户注意力转移的“流量传导行为”本身就具有讨论价值。不过，由于不成功的流量传导行为难以为平台带来经济利益，无法据此论证平台市场力量的强化路径，故本文不对此展开论述。

（二）算法分析提高流量利用率

流量是用户注意力的具象化，数字经济平台实施流量传导行为的目的在于吸引用户注意力，获取更多的交易机会。但正如前文所述，流量传导行为的效果具有不确定性：既可能导致用户完全抛弃一个平台而转向另一个平台，也可能只是短期的吸引用户而不能达到较高的用户黏性；既可能使用户接受推广并进行消费，也可能遭到用户的拒绝和反感。概言之，流量传导行为所带来的交易机会的大小不能一概而论。特别是在缺乏算法分析的情况下，传导来的流量很可能与接受传导方的需求缺乏匹配度，从而使得接受传导一方的目的落空。

导流效果的不确定性，在一定程度上减损了流量利用的价值。在没有进行算法分析的情况下，单纯的流量传导行为虽然能够带来用户的注意力，但此种注意力的经济价值不能被很好地挖掘和评估。有学者提出，流量的价值在于“转化率”。如用户对广告的注意力转化为广告产品的购买量，体现了用户输入型流量的价值。百度用户输入的搜索词，可以成为百度市场需求分析的数据源，体现了用户输出型流量的价值。〔21〕没有经过加工和匹配的流量，其价值难以被准确衡量，既不利于实现流量的价值转化，从长远看也不利于流量传导交易的开展。

---

〔19〕 See Wu T，Blind Spot：The Attention Economy and the Law，82 *Antitrust Law* Journal，771（2018－2019）.

〔20〕 参见刘佳欣：《反不正当竞争法视角下的流量劫持——以流量劫持典型案例为分析样本》，载《法律适用》2019 年第 18 期。

〔21〕 参见王潺：《互联网不正当竞争法律评价的法经济学分析》，载《广东财经大学学报》2020 年第 6 期。

算法与流量结合才能够实现平台市场力量的拓展。平台作为数据集合体的中心，天然就具有利用算法进行分析的需求。〔22〕精确匹配的算法极大提高了流量价值的转化率，有利于加强流量利用的确定性。从算法分析发挥流量价值的实现路径考量，可以发现，算法对流量价值的挖掘主要从两个维度进行。

其一，数字平台通过算法分析，能“预测用户偏好、支付意愿、最高保留价格，设计目标用户群精密的差别定价、数据利用的个性化服务”〔23〕，以提高自身对市场和用户行为的预判力，从而确定经营战略。换言之，企业对消费者的了解越多，就越能够更好地满足消费者需求，将他们与他们可能喜欢的内容相匹配，促使消费者支付更多，实现注意力的货币化。〔24〕有学者将这一实现路径称为“用户反馈回路”。通过此种反馈循环还可以产生规模经济，即当平台拥有大量用户，获得更多的用户数据时，就能更好地洞察消费者需求，进而提高服务质量以吸引更多用户。〔25〕

其二，算法分析除了能预测用户偏好、提升平台的服务质量之外，还可以实现更为精准的广告投放，使平台获得更多的在线广告收入，促进流量价值的变现。互联网广告是互联网平台的基本盈利模式之一，对于不直接通过销售产品获取利润，或不以平台销售为主要发展方向的平台而言，提供推广服务、获取广告收入往往是其利润的主要来源。当前，数字经济时代的发展已经给广告行业带来了日新月异的变化，广告主从漫无目的的量化式投放，过渡到更倾向于精准到消费者个人的精细化投放。能够满足广告主这一需求的平台无疑会更受青睐，获取更多的广告服务机会，收取更高的广告推广费用。

（三）流量优势转化为数据优势

对数字经济平台而言，流量和数据有着密不可分的关系。平台本质上就是流量入口的数据集合体，它以数据生产要素为核心，通过算法设计与操作创造市场价值，驱动平台、数据、算法三维结构的市场竞争新格局。〔26〕一方面，流量是数据的来源和基础，用户的每一次浏览和点击都会在平台上留下自己的痕迹。平台在取得用户许可的前提下可以对这些痕迹进行收集和加工，实现流量到数据的转化。从这个角度来看，流量传导的过程也可以被看作数据积累的过程。另一方面，流量传导行为可以为平台带来新的用户和关注度，从而提高平台所收集的数据的更新速度。在数据时效性凸显的数字经济时代，能够较快地更新数据无疑是平台保持自身竞争力的关键。

当然，流量与数据在价值层面上也存在显著的差异。其一，动态的流量传导固然具有财产价值，但是由于传导的效果不能确定且难以衡量，在这个环节难以明确其价值。而当流量传导带来的数据积累完成后，流量价值会转变为数据价值，其将更为客观、易于感知。其二，流量传导的价值主要体现在传导者和被传导者之间，其往往是一种商业行为，普通用户难以分享这一行为产生的价值。相较而言，数据价值则更可能被广泛分享，因为数据生成是由用户行为带来的，用户对其所提供的数据内容有一定控制力。或许在将来可以通过发行“共票”的方式使互联网用户也

〔22〕 参见杨东：《论反垄断法的重构：应对数字经济的挑战》，载《中国法学》2020 年第 3 期。

〔23〕 杨东、臧俊恒：《数字平台的反垄断规制》，《武汉大学学报（哲学社会科学版）》2021 年第 2 期，第 165 页。

〔24〕 See Ryan Calo，Alex Rosenblat，The Taking Economy：Uber，Information，and Power，117 *Columbia Law Review*，1623－1690（2017）.

〔25〕 参见贾晓燕、封延会：《网络平台行为的垄断性研究——基于大数据的使用展开》，载《科技与法律》2018 年第 4 期。

〔26〕 参见前引〔23〕，杨东、臧俊恒文。

能分享数据价值。〔27〕

平台为增强其市场力量，往往会将自身的“流量优势”转化为“数据优势”，以尽量多获取、更好利用“数据”这一生产要素，并借此拓展自身的市场力量。“流量优势”向“数据优势”的转化会加剧数字经济平台领域的“赢者通吃”现象。从经济学角度分析，使用两种竞争产品的边际成本大于收益时，就可能发生市场的单一导向。〔28〕对平台而言，当其掌握了大量流量时，用户在该平台及其提供导流服务的平台上满足需求的成本更低也更为便利，因此会更倾向于使用这些服务。当流量和数据随着用户的聚集而聚集在少数互联网巨头手中时，就会形成数字经济平台领域的“赢者通吃”现象。〔29〕关于平台如何利用流量传导行为增强其在本市场和其他市场上的力量，本文将在下一部分以社交平台为例予以详细论述。

三、流量传导行为增强平台市场力量的实例分析

鉴于流量的无体性和传导的便捷性，流量传导的作用范围不受时间和地域的限制，其既可以扩大平台在其他市场上的影响力，也能够增强平台在同一市场上的力量。以社交平台的流量传导为例，由于流量对短视频市场的发展具有必要性，封禁 API 等拒绝流量传导的行为引起了抖音与腾讯的纠纷。反观之，社交平台的流量传导行为也可以将其本身的影响力传递到短视频市场上，微信“视频号”的发展就是一个例证。另外，社交平台通过流量传导能够增强自身在同一市场上的力量。具体而言，流量传导可以助力平台转型以延续其优势地位。相反，若缺乏导流，社交网络的强锁定效应会使新的市场进入者难以挑战之前平台的地位。

（一）借助流量传导行为增强自身在其他市场的力量

积聚海量用户、掌握流量入口的社交平台具有天然的流量优势。中国社会科学院大学互联网法治研究中心在《互联网平台与数据竞争规制问题研究报告》中提出，社交软件的影响力已超越了单纯的私人社交属性，而带有商业交易上的“交往”属性。目前，各行业的经营者正越来越将社交平台作为经营、推广、引流的工具。以腾讯为例，鉴于其旗下的微信和 QQ 几乎独占了国内社交软件平台的流量，诸多企业选择与腾讯合作换取更大的发展机会。基于自身的流量优势，腾讯对其“合作伙伴”的控制度也逐渐加深，以其为中心的新型互联网垄断正在形成。〔30〕

区别于传统企业在实体经济中的垄断，“流量垄断”成为数字经济时代屡见不鲜的现象，与其相关的纠纷也随之显现。2021 年 2 月 2 日，字节跳动旗下的抖音在北京知识产权法院向腾讯提起反垄断诉讼。其提出，微信、QQ 以“短视频整治”为由，对抖音等产品进行了长达三年的持续封禁和分享限制。这一行为构成《反垄断法》所禁止的“滥用市场支配地位排除、限制竞争的垄断行为”。〔31〕腾讯则发布声明回应称，字节跳动公司的相关指控纯属失实，系恶意诬陷，且字

〔27〕 参见杨东：《“共票”：区块链治理新维度》，载《东方法学》2019 年第 3 期。

〔28〕 See Hovenkamp，Herbert J，*Antitrust and Platform Monopoly*，Legal Scholarship Repository：Faculty Scholarship at Penn Law，2020，p. 1924.

〔29〕 参见杨东：《后疫情时代数字经济理论和规制体系的重构——以竞争法为核心》，载《人民论坛·学术前沿》2020 年第 17 期。

〔30〕 参见朱邦凌：《微信收费的“底气”在于“新流量垄断”》，载《新京报》2018 年 7 月 3 日，第 B02 版。

〔31〕 参见《关于抖音起诉腾讯垄断的声明》，载微信公众号“抖音”，2021 年 2 月 2 日。

节跳动及相关公司存在诸多侵害平台生态和用户权益的违法违规行为。〔32〕

“头腾大战”的争议主体抖音属于短视频平台，微信和 QQ 则属于社交平台。二者固然处于两个不同的市场，但“流量”如同一个管道，可以将两个市场连通起来。流量对致力于吸引大量用户积极创作、分享和交流的短视频市场来说，具有重要意义。甚至可以认为，流量是短视频应用发展的基础。腾讯关闭 API 接口导致某些抖音用户无法通过社交平台网络授权登陆，或无法通过直接跳转分享链接等内容到社交平台，实际上是拒绝为抖音提供流量传输途径，切断了流量传导的管道。这将会使抖音用户登录、分享的步骤复杂化，影响到抖音用户的分享积极性。从反垄断法的视角来看，腾讯是否构成垄断还需经进一步分析。但就其行为本身而言，“拒绝向竞争者开放数据入口”已被认为是具有数字经济特征的新型垄断行为。〔33〕 关闭 API 接口作为一种平台封禁行为，可能会涉嫌违反反垄断法关于排他性交易、拒绝交易、差别待遇等的规定。〔34〕

社交平台的流量封禁会影响短视频应用的发展，反观之，社交平台的流量传导行为也可以将其本身的影响力传递到短视频市场上。实际上，腾讯自身也关注到了短视频市场的潜力，早已将短视频作为自己的主要进攻方向之一。据三言财经统计，腾讯至少上线了微视、企鹅看看、闪咖、QIM、DOV、MOKA 魔咔、猫饼等约 16 款短视频相关 APP，再加上依托微信平台的时刻视频，短视频产品的总数约 17 个。2020 年 1 月 19 日微信的视频号上线，2020 年 6 月，微信官方宣布视频号日活已破两亿。方正证券预测在没有开启商业化的情况下，视频号目前的日活基准水平是 3 亿，长期空间预估 6 亿，最终会接近微信本身的日活水平。〔35〕

数字平台通过对流量入口的垄断，将自己变成了行业和社会的中心，并借助流量合作加深对其他经营者的控制。可以认为，平台利用自身海量、高黏性的流量调控和分配，在与其紧密合作的经营者之间构建起了基于流量的卡特尔，〔36〕 通过导流行为增强了自身在其他市场上的力量。

（二）借助流量传导行为增强自身在同一市场的力量

2021 年 1 月，米聊发布公告称，其将于 2021 年 2 月 19 日停止服务。而与其发布时间相近、功能相似的竞争对手微信，如今已成为国民级的社交通信产品。2021 年 3 月 24 日，腾讯发布 2020 年第四季度业绩报告。宣布微信用户已逾 12 亿，每天超过 1.2 亿用户在朋友圈发表内容，3.6 亿用户阅读公众号文章，4 亿用户使用小程序。〔37〕 回顾历史可以发现，微信的成功并非一帆风顺。其上线半年后，用户数还未达到 100 万。而当时，腾讯 QQ 注册用户已超过 6 亿，成为腾讯在移动社交领域的护城河。〔38〕 为支持微信的发展，腾讯作出决定通过 QQ 为微信导流。一方面，QQ 在其主页和 QQ 邮箱的首页打出了微信的广告，吸引用户关注这一新产品；另一方面，QQ 为微信提供了互操作性，方便用户从 QQ 转移至微信。相比通过通讯录添加好友的米聊，微信用户可以通过 QQ 账号注册，且微信可读取 QQ 好友的信息，并将他们添加至好友列表。正是

〔32〕 参见《字节跳动恶意构陷，腾讯将起诉》，载微信公众号“鹅厂黑板报”，2021 年 2 月 2 日。

〔33〕 参见刘云：《互联网平台反垄断的国际趋势及中国应对》，载《社会科学文摘》2021 年第 2 期。

〔34〕 参见张江莉、张镭：《互联网“平台封禁”的反垄断法规制》，载《竞争政策研究》2020 年第 5 期。

〔35〕 参见《微信的生态与野望：大音希声，大象无形》，载微信公众号“方正证券研究”，2021 年 1 月 20 日。

〔36〕 参见前引〔23〕，杨东、臧俊恒文。

〔37〕 参见《腾讯发布 2020 年业绩报告，全年净利润 1598.5 亿元人民币》，载 https：//www.chinaz.com/news/1231338.shtml，最后访问时间：2021 年 4 月 27 日。

〔38〕 参见《微信十年，“熬死”一个又一个对手》，载 http：//www.chinanews.com/cj/2021/01-26/9396867.shtml，最后访问时间：2021 年 4 月 27 日。

通过 QQ 一系列的导流措施，微信才能在短期内获取大量用户，上线 433 天即实现了用户数突破 1 亿，在同时期推出的同类社交产品中脱颖而出。

不同网络间的高转换成本所带来的锁定效应，在社交网络中表现得更为明显。这意味着，在缺乏外因干涉的情况下，用户大量从一个已成熟的社交平台向另一个平台转移的可能性较低。相反，如果用户关系链上的相当一部分用户选择了另一个平台，则该用户也有很大可能向该平台转移。有学者曾指出，用户使用移动 SNS 的行为意愿强烈依赖于社会影响、群聚效应。〔39〕还有学者归纳出了三段式社交媒体用户转移行为路径，指出用户在过渡阶段的转移，大部分是由于受到了周围环境的影响和带动。〔40〕从这一理论出发看 QQ 为微信导流事件，可以发现，QQ 实施流量传导的行为，特别是为微信提供互操作性，可以有效地降低用户转移成本，弱化 QQ 本身的锁定效应。又由于 QQ 导流对象的唯一和确定性，弱化 QQ 锁定效应带来的流量红利只能由微信享有，这为微信的早期发展提供了机遇。

从深层意义上看，QQ 的流量传导不仅助力了微信的发展，更重要的是，其帮助腾讯实现了在社交应用领域的成功转型。QQ 的设计是基于 PC 时代的用户体验，由于当时的技术水平有限，PC 端的 QQ 移植到手机端时，无法复制全部功能，且数据无法做到同步。另外，QQ 的用户定位在年轻人群体，功能上更偏向娱乐化，受众有限，且由于每个用户可以注册的 QQ 号数量缺乏限制，导致有些 QQ 号实际上长期处于无人使用的低活跃度状态，不利于 QQ 进一步发展用户。在米聊等竞争对手纷纷推出竞争性产品之际，为了在手机端占据市场、实现自身在社交应用领域的转型，腾讯选择利用 QQ 导流微信，借此占据了更大的市场份额，增强了自身在同一市场上的力量。

流量传导行为可以助力平台转型以保持优势地位，反之，在缺乏导流的情况下，网络特别是社交网络的强锁定效应会凸显出来。这意味着，在同一个市场已存在基本成熟的平台时，与其功能互补性不强的平台将很难争取用户的关注，也因此无力挑战之前平台的优势地位。当前微信几乎独占了国内社交软件平台的流量。由于用户在微信上的好友、聊天记录、朋友圈等无法打包转移到其他社交软件平台，社交应用领域用户的低迁移度制约了同类社交软件的发展，遑论与微信相抗衡。实际上，在社交应用市场上，若缺乏腾讯系的导流，锁定效应会将网络访问变成竞争性武器。〔41〕如快播的马桶 MT、字节跳动的多闪、锤子科技的聊天宝，虽都定位于社交，想要挑战微信的地位，但在发布伊始，三个 APP 就都遭到了微信的屏蔽，其流量巅峰也只出现在刚推出之时。

四、余　论

数字经济平台实施的流量传导行为能够增强平台的市场力量，而且其作用范围不受时间和地域的限制。平台市场力量的增强无疑会引发人们关于垄断风险的担忧，鉴于预防和制止垄断行为是语

〔39〕 See Shahrokh Nikou，Harry Bouwman，Ubiquitous use of mobile social network services，31 *Telematics and Informatics*，422－433 (2014).

〔40〕 参见贾若男、王晰巍：《基于扎根理论的社交媒体用户转移行为特征研究》，载《图书馆学研究》2018 年第 17 期。

〔41〕 参见李勇坚、夏杰长：《数字经济背景下超级平台双轮垄断的潜在风险与防范策略》，载《改革》2020 年第 8 期。

序逻辑下《反垄断法》的首要立法目的，〔42〕因此流量传导行为有必要受到《反垄断法》的审视。

规制平台流量传导行为的路径有两条。其一是将其作为垄断行为的一种规制。但流量传导服务协议不能被认为是一种“垄断协议”，其如果配合流量垄断行为实施，固然可能会加剧“流量垄断”的反竞争效果，如腾讯封禁抖音的同时大力推广其自身的“视频号”功能，有效抢占了短视频市场，但仅凭流量传导行为，很难达到垄断协议所要求的排除、限制竞争的效果。且流量传导行为也不符合《反垄断法》中“滥用市场支配地位”的行为样态。第二种选择是将其作为认定平台“市场支配地位”之有无的考虑因素。认定互联网平台经营者具有市场支配地位，应同时考虑平台的经营模式、网络效应、经营者掌握和处理相关数据的能力、经营者在关联市场的力量等因素。流量传导行为在很大程度上反映了平台的经营模式，且能够增强网络效应、为经营者提供持续的数据流，通过杠杆效应增强经营者在关联市场的力量。因此在认定平台市场支配地位时，有必要考虑到其流量传导行为的实施情况。

总而言之，流量传导的价值不可低估，有必要对其进行规范，正确引导流量价值的实现。在规范流量传导行为时，应注意避免引发垄断风险，保持互联网的开放共享性。在判断平台企业是否具有市场支配地位时，应将其进行流量传导的能力、流量传导行为的有无以及效果纳入考量因素。

Abstract：Flow conduction behavior is not equivalent to purely data transmission or agglomeration，and it is significant to discuss this behavior separately from data. Because the forms of flow conduction behavior on the platform are different with various business models of platforms，it should be analyzed in diverse scenarios. From the macro level，the flow conduction behavior makes the leverage effect easier to achieve，and raises the market entry barriers. As a result，there is a conclusion that the flow conduction behavior can enhance the market power of the platform. From the perspective of specific implementation path，the direct impact of flow conduction behavior on the platform is to bring flow，that is，users’ attention. The accurate matching algorithm greatly enhances the conversion rate of flow value and strengthens the certainty of flow utilization. Moreover，the process of flow conduction is also the process of data accumulation. By improving the update speed of data，it helps the platform transform the advantage of flow into advantage of data，and intensifies the “winner takes all” phenomenon in the platforms of digital economy.

Key Words：flow conduction behavior，platform，market power，monopoly

（责任编辑：殷秋实　赵建蕊）

〔42〕 参见刘乃梁：《“预防垄断行为”的理论逻辑及其制度展开》，载《社会科学》2020 年第 12 期。

财经法学 No. 2，2022
pp. 146 - 162

论算法个性化定价的解构与规制
——祛魅大数据杀熟

雷　希*

内容提要：算法个性化定价的监管实践与理论分析未能遵循规制对策与问题相匹配的规制原理。该原理要求注意算法个性化定价与算法合谋定价、欺诈定价、歧视定价、个性化推荐的区别。同时基于危害性差异我们也应将算法个性化定价进一步分为三类：超高价格、超低价格和一般价格。超高价格或超低价格场景下的算法个性化定价危害可借助既有的法律框架得以消减。虽然一般价格场景下的算法个性化定价既没有损害消费者权益，也不会排除或限制竞争，但会从分配不公平和程序不公平两个角度诱发消费者不信任，动摇数字市场经济秩序。政府、经营者和消费者应以信任受损机理为基本遵循，合力共筑消费者信任，以实现创新发展和消费者利益保护的动态平衡。

关键词：大数据“杀熟”　算法个性化定价　分类规制　消费者信任

大数据“杀熟”已引起社会的广泛关注，社会各界曾强烈呼吁政府通过加强立法工作治理大数据“杀熟”现象，堵住监管漏洞。〔1〕《个人信息保护法》第24条被普遍解读为禁止大数据“杀熟”，〔2〕各地出台的地方性法规及规范性文件也对此作出了规定。〔3〕大数据“杀熟”又被称为算法价格歧视、个性化定价或差异化定价等，是公众对经营者利用算法为终端消费者个性化定价的一种俗称，即通过收集、清洗、处理和分析消费者消费习惯、消费能力等个人信息对消费者画像，预测消费者最高保留价格，并以此就同一商品向条件相同的消费者设定高低不同的价格。大

* 雷希，南京大学法学院博士研究生。

本文为国家社科基金一般项目“数字经济背景下企业数据权属及利用规则研究”（20BFX122）的阶段性成果。

〔1〕 参见《全国人大代表杨松：建议立法规制大数据杀熟、平台二选一等》，载 https://www.thepaper.cn/newsDetail_forward_11533557，最后访问时间：2022年1月5日。

〔2〕 参见王利明：《〈个人信息保护法〉的亮点与创新》，载《重庆邮电大学学报（社会科学版）》2021年第6期；王利明、丁晓东：《论〈个人信息保护法〉的亮点、特色与适用》，载《法学家》2021年第6期。

〔3〕 如《上海市数据条例》《深圳经济特区数据条例》《浙江省电子商务条例》等。

数据“杀熟”并非学术用语，其主观色彩过于浓厚。如果用大数据“杀熟”指称这类行为则易形成框架效应（framing effect），导致立场先行，〔4〕不利于对此进行中立评价。〔5〕鉴于概念的使用还未有共识，且国内外不少学者也以算法个性化定价来指称该类行为，因此本文采用算法个性化定价来代替大数据“杀熟”这一用语。

国内外监管机关和理论界基于保护消费者、弥补市场失灵的目的，基本认可政府应采取措施规制算法个性化定价。〔6〕但难点在于应该如何规制算法个性化定价、既有法律框架是否足以解决算法个性化定价带来的挑战。对该类问题的理论研究，既是回应社会重大关切的现实之需，也是数字经济发展之求。

一、既有监管与理论的特点归纳及缺陷分析

我国目前对算法个性化定价的监管思路呈现出一刀切禁止的特点，国内理论研究则呈现出一般化分析的特点。一刀切禁止的监管思路和一般化的理论研究均存在不足，有待进一步完善。

（一）监管一刀切禁止的特点与缺陷

有关算法个性化定价的国内监管呈现出一刀切禁止的特点，即以统一适用的禁止性规范规制涉及算法个性化定价的所有问题。例如，2021 年国家市场监督管理总局、中央网信办、国家税务总局提出必须“严肃整治”算法个性化定价。国务院反垄断委员会制定的《关于平台经济领域的反垄断指南》第 17 条，被认为是对算法个性化定价这一热点问题的回应。〔7〕《价格违法行为行政处罚规定（修订征求意见稿）》将算法个性化定价视为“新业态中的价格违法行为”，明确将按销售总额比例罚款。类似一刀切禁止性的规定还有不少。〔8〕结合违法惩戒机制，这种一刀切禁止的监管思路具有较强的威慑力。

一刀切禁止的思路有很强的民意及舆论基础。如 2019 年北京市消协的调研结果显示，绝大多数被调查者（83.74%）认为算法个性化定价侵犯了消费者公平交易权，类似比例的被调查者（81.41%）要求政府加强监管以减少此类行为。〔9〕除此之外，一刀切禁止还可以为将来的灵活

〔4〕 See Ariel Ezrachi, Maurice E. Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Harvard University Press, 2016, pp. 111 - 113.

〔5〕 笔者于“中国知网”搜索相关 CSSCI 论文发现：一般而言，采用大数据杀熟或算法歧视这类表述的文章，基本假定算法个性化定价攫取消费者剩余，限制竞争，应该予以规制；而采用中立性表述的文章一般认为算法个性化定价危害性较为复杂，需要结合不同场景进行分析。

〔6〕 参见喻玲：《算法消费者价格歧视反垄断法属性的误读及辨明》，载《法学》2020 年第 9 期；Organisation for Economic Co-operation and Development（OECD），Price Discrimination：Background Note by the Secretariat，DAF/COMP（2016）15.

〔7〕 参见《促进平台经济规范有序创新健康发展 ——〈国务院反垄断委员会关于平台经济领域的反垄断指南〉解读》，载 http://gkml.samr.gov.cn/nsjg/xwxcs/202102/t20210207_325970.html，最后访问时间：2022 年 1 月 5 日。

〔8〕 例如《商务部办公厅开展“2021 年全国网上年货节”活动的通知》、文化和旅游部《在线旅游经营服务管理暂行规定》、国家市场监督管理总局联合商务部共同提出“社区团购‘九不得’”、国家互联网信息办公室《数据安全管理办法（征求意见稿）》等。

〔9〕 参见《北京市消协发布大数据“杀熟”问题调查结果》，载 http://www.bj315.org/xxyw/xfxw/201907/t20190727_19494.shtml，最后访问时间：2022 年 1 月 5 日。

规制预留充足时间，〔10〕在短时间内也可以为市场注入一剂强心针。

但一刀切禁止的处理方法只能是一时的应对之策。相较于包容审慎监管，一刀切禁止所能获得的效益小于增加的成本。〔11〕更为重要的是，算法个性化定价的经济效果较为复杂，对经营者、消费者及社会也会带来一定程度的正面效应。英国竞争与市场监管局（CMA）2021 年发布研究报告指出，算法个性化定价尽管有时会损害消费者利益，甚至侵蚀整体经济效率，但有时也能够增加消费者福利。〔12〕一味禁止个性化定价，会使得个案处理欠缺灵活性，〔13〕从长远来看甚至还会损害消费者权益〔14〕。一刀切禁止的实效也不容乐观。CMA 调查发现天然气与电力市场办公室（Ofgem）2009 年禁止区域差异化定价的决定并未产生促进竞争的效果，相反还弱化了竞争。〔15〕

综上，对算法个性化定价的监管不宜采用一刀切禁止的思路。〔16〕近期出台的《个人信息保护法》《互联网信息服务算法推荐管理规定》和《浙江省电子商务条例》等规定仅禁止“不合理”的算法个性化定价，试图从一刀切禁止的监管策略转变为合理分析。但这些规定并未明确“不合理”的概念，这就要求监管者进行个案分析。然而由于监管能力与监管成本的约束，监管者在个案的实际判断中可能仍会偏向于一刀切处理。这意味着，尽管部分监管规范的表述由禁止转为合理分析，但其实践效果没有发生变化，市场活力可能仍会受挫。

（二）理论一般化分析的特点与缺陷

国内对算法个性化定价的研究呈现出“一般化”的特点，也就是将所有危害都归因于算法个性化定价这个一般性概念上，未区分不同情形下算法个性化定价的危害差异。具体表现为：其一，有的研究断言算法个性化定价不仅可能攫取消费者剩余，而且还可能扭曲市场竞争机制，排除限制竞争。〔17〕其二，有的研究从不同部门法角度讨论算法个性化定价的危害性，意图为一般性禁止算法个性化定价提供具体条文依据。例如从消费者保护法的角度，有观点认为算法个性化定价侵犯消费者知情权、选择权或公平交易权；〔18〕从反垄断法的角度，有观点认为算法个性化定价构成剥削性差别待遇；〔19〕从行政行为法和行政作用法视角，也有学者讨论规制算法个性化定价的理论正当性〔20〕。前述部门法视角的讨论仍旧将所有可能的危害笼统地归咎于算法个性化

〔10〕 有研究发现，政府强监管的初始意愿越强烈，互联网企业演化到算法个性化定价的速度越慢。参见邢根上、鲁芳、罗定提：《政府监管下的电商大数据“杀熟”演化仿真分析》，载《湖南工业大学学报》2021 年第 2 期。

〔11〕 参见潘定、谢菡：《数字经济下政府监管与电商企业“杀熟”行为的演化博弈》，载《经济与管理》2021 年第 1 期。

〔12〕 See Competition & Markets Authority（“CMA”），Algorithms：How They Can Reduce Competition and Harm Consumers，Jan. 19，2021，pp. 8－9，available at https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers，last visited on Jan. 5，2022.

〔13〕 参见宋亚辉：《社会性规制的路径选择：行政规制、司法控制抑或合作规制》，法律出版社 2017 年，第 164－165 页。

〔14〕 See Alex Schofield，Personalized Pricing in the Digital Era，18 *Competition Law Journal*，35，40（2019）.

〔15〕 See CMA，Energy Market Investigation，Final Report，Jun. 24，2016，available at：https://assets.publishing.service.gov.uk/media/5773de34e5274a0da3000113/final-report-energy-market-investigation.pdf，last visited on Jan. 5，2022；OECD，Personalised Pricing in the Digital Era-Note by the United Kingdom，p. 12，DAF/COMP/WD（2018）127.

〔16〕 参见李毅、李振利：《数字经济背景下对消费者实行个性化定价违法边界的研究》，载《社会科学》2020 年第 2 期。

〔17〕 参见李丹：《算法歧视消费者：行为机制、损益界定与协同规制》，载《上海财经大学学报》2021 年第 2 期。

〔18〕 参见王佳琪：《大数据“杀熟”的法律应对》，载《人民法院报》2019 年 6 月 11 日，第 002 版。

〔19〕 参见杨东、臧俊恒：《数字平台的反垄断规制》，载《武汉大学学报（哲学社会科学版）》2021 年第 2 期。

〔20〕 参见李帅：《共享经济信息不对称环境下的决策算法规制——以区块链共识模型为规制思路》，载《财经法学》2019 年第 2 期。

定价，未能进行场景化和类型化分析。当然，确实也有学者尝试进行类型化分析。有的主张“对于不同类型的个性化定价算法应做区分处理”〔21〕，有的认为应“基于消费者细分的视角”坚持个案分析〔22〕。这些观点虽然意识到算法个性化定价在不同条件下呈现出不同效果，但也仅是一般性地提及个案分析中应考虑的原则，尚未落实如何分类规制。

一般化分析兼具进步之处与不足之处。其进步之处包括：一是明确算法个性化定价可能的危害性，解决了规制必要性问题；二是提出算法个性化定价的综合规制进路，并试图深入到各部门法领域进行研究。

缺陷之处则体现在三个方面。第一，既有研究未能意识到算法个性化定价并非独立概念，其外延并非独一无二，而是包含多种具有不同危害性的子类行为。一般化分析将算法个性化定价视为一个整体进行研究，遇到具体场景时便会暴露出解释力不足的问题。第二，一般化分析容易混淆算法个性化定价子类行为的危害，可能产生规制错配的问题。例如，有观点将特定类型算法个性化定价对消费者权益的损害视为算法个性化定价共有的特征，进而主张通过援引“维护消费者利益”这个一般条款而适用《反垄断法》规制所有算法个性化定价。〔23〕然而，有些类型的算法个性化定价既不损害消费者权益，也不排除限制竞争，此时如果《反垄断法》介入势必会导致规制错配。第三，一般化分析未能遵循问题与对策相匹配的规制原理，未能厘清不同场景下的算法个性化定价的危害差异，未能据此构建规制进路。

二、基于危害差异的类型化研究

针对上述缺陷，改进方法是围绕算法个性化定价不同子类行为的危害差异进行类型化处理，从而为具体规制路径的建构奠定基础。

（一）理据与功能分析

以危害性差异为基础进行类型化研究不仅可用规制理论来论证其正当性，而且也因其多重价值而具有必要性。

第一，类型化研究根源于规制路径应与问题相匹配的基本原理。算法个性化定价的规制路径选择具有鲜明的实用主义色彩，无论如何设计规制路径（是自由放任，抑或照搬或准用既有法律规定，甚或是重建），都必须遵循对策与问题相匹配的规制原理。〔24〕否则可能产生规制失败、规制错配等问题。〔25〕

〔21〕 周围：《人工智能时代个性化定价算法的反垄断法规制》，载《武汉大学学报（哲学社会科学版）》2021 年第 1 期，第 108、110 页。

〔22〕 参见喻玲、兰江华：《算法个性化定价的反垄断法规制：基于消费者细分的视角》，载《社会科学》2021 年第 1 期。

〔23〕 参见承上：《人工智能时代个性化定价行为的反垄断规制——从大数据杀熟展开》，载《中国流通经济》2020 年第 5 期。

〔24〕 参见宋亚辉：《网络市场规制的三种模式及其适用原理》，载《法学》2018 年第 10 期。

〔25〕 参见〔美〕史蒂芬·布雷耶：《规制及其改革》，李洪雷、宋华琳、苏苗罕、钟瑞华译，北京大学出版社 2008 年版，第 277 页及以下。

第二，基于危害差异解构算法个性化定价具有多重价值。首先，解构算法个性化定价可以弥补一刀切禁止和一般化分析的缺陷。类型化的思考有助于我们清楚地掌握算法个性化定价的多种类型，避免将不同危害混为一谈；更有助于对算法个性化定价进行规范分析，探寻不同法律在算法个性化定价场景下的适用空间。其次，类型化的分析可以辅助判断是否存在规制失败，进而便于查漏补缺。最后，类型化分析相较于个案分析具有节省成本、提高法律确定性的作用。个案分析的优点是可以基于个案具体情况灵活选择不同的规制进路，但缺点在于耗时耗力，且无法给市场主体稳定的行为预期。通过类型化分析，事先明确各类算法个性化定价的规制路径，能够发挥法律规则的行为指引作用。

（二）解构算法个性化定价

算法个性化定价存在多种表现形式，各种表现形式的危害存在差异，应据此探寻算法个性化定价的类型。但在此之前，有必要厘清算法个性化定价与相关概念的差异。因为尽管算法个性化定价的内涵与相关概念的内涵不同，危害性也迥异，但目前的研究存在概念混淆的问题，有碍规制路径的构建。

1. 厘清算法个性化定价内涵

第一，应注意区分算法个性化定价与个人信息保护问题、“信息茧房”困境。按照行为机制，利用算法技术实施个性化定价的行为可以分为信息采集、信息推送、个性化定价三个阶段。〔26〕这三个阶段的行为表现及危害性各不相同。信息采集阶段主要涉及个人信息知情同意、用户画像、隐私侵权等问题，信息推送阶段的主要危害在于信息茧房，算法个性化定价是发生在第三个阶段的行为。然而，有些研究混淆了上述三个阶段的危害。例如，有观点认为算法个性化定价因为违背了消费者对数据及隐私的实质期待而是不公平的；〔27〕也有观点将信息个性化推送归类为“大数据杀熟”，〔28〕还有观点试图通过解释《电子商务法》第 18 条第 1 款关于个性化推送的规定以解决算法个性化定价问题〔29〕。本文认为，在建构算法个性化定价的规制路径时，不能混淆算法个性化定价与信息采集阶段的个人信息保护问题、信息推送阶段的“信息茧房”问题。用《个人信息保护法》第 24 条禁止算法个性化定价可能有违《个人信息保护法》的规制逻辑，不仅可能会使得相关规定泛化，〔30〕还会造成规制错配。这是因为算法个性化定价的成因并非个人信息保护不足，〔31〕《个人信息保护法》可提高个人信息保护水平，但很难对算法个性化定价形成有效规制。

〔26〕 参见前引〔17〕，李丹文。

〔27〕 See Christopher Townley, Eric Morrison, Karen Yeung, Big Data and Personalized Price Discrimination in EU Competition Law, 36 *Yearbook of European Law*, 683, 710 - 711 (2017).

〔28〕 参见郑智航、徐昭曦：《大数据时代算法歧视的法律规制与司法审查——以美国法律实践为例》，载《比较法研究》2019 年第 4 期。

〔29〕 参见付丽霞：《大数据价格歧视行为之非法性认定研究：问题、争议与应对》，载《华中科技大学学报（社会科学版）》2020 年第2 期。

〔30〕 参见文铭、莫殷：《大数据杀熟定价算法的法律规制》，载《北京航空航天大学学报（社会科学版）》，2021 年 9 月 18 日网络首发。

〔31〕 参见李三希、武玙璠、鲍仁杰：《大数据、个人信息保护和价格歧视——基于垂直差异化双寡头模型的分析》，载《经济研究》2021 年第 1 期。

第二，应注意区分算法个性化定价和其他价格违法行为，比如算法合谋定价、算法欺诈定价、算法歧视定价。首先，个性化定价与合谋定价差异明显。个性化定价的特点在于价格存在较大差别，而合谋定价的特点在于价格一致，两者表现形式不同。尽管算法可能辅助经营者就同一消费者达成统一动态价格，但尚未有足够证据证明这已成为现实。〔32〕算法合谋定价行为可由《价格法》第14条第1项或《反垄断法》予以规制。其次，个性化定价并非欺诈定价，这是因为欺诈需要有误导性陈述，而个性化定价并不会使消费者陷入双重错误。那些认为算法个性化定价构成价格欺诈的观点，〔33〕混淆了个性化定价与欺诈定价。算法欺诈定价可由《民法典》以及《消费者权益保护法》第20条和第55条予以规制。最后，算法歧视定价是平等权语境下的概念，体现为针对性别、种族等身份方面的歧视定价，可通过“反歧视法律数字化转型”得以解决。〔34〕

2. 解析算法个性化定价外延

根据危害性差异，可将算法个性化定价的外延解构为三个非空的子类：超高价格、超低价格和一般价格。这三类行为囊括了算法个性化定价的所有类型。

（1）超高价格

超高价格是指明显高于商品或服务市场价值的价格。市场交易本应是平等互惠互利的。超高价格的潜在危害在于导致交易显失公平，侵害消费者福利。经营者利用数据与算法探知消费者的价格极限，向高支付意愿的消费者收取超高价格，过度剥夺了这部分消费者剩余，使得交易难以对消费者产生增益。超高价格还使得消费者与经营者之间的付出与收益不成比例，损害了实质公平。例如在浙江省绍兴市柯桥区法院审理的胡女士诉上海携程商务有限公司侵权纠纷一案中，胡女士通过“携程”订购房间的价格为2889元，而通过线下预定则仅为1377.63元，〔35〕此时价差达到了一倍，应属于超高价格。

（2）超低价格

超低价格是明显低于商品或服务市场价值的价格。利用算法设定过低价格可能排除限制竞争、扰乱正常经营秩序。经营者通过差异化定价向高支付意愿的消费者收取较高利润，以此补贴低支付意愿的消费者，利用低价留住这部分消费者，或吸引新消费者。当经营者持续地以超低价格销售商品或提供服务，便很可能会产生扰乱正常经营秩序的效果。在经营者处于市场支配地位时还会产生排除限制竞争的效果。利用算法设置超低价格的行为在经济生活中确有可能发生。〔36〕例如，“多多买菜”“美团优选”等社区团购便被爆出采取补贴的方式低价竞争，甚至个别产品远低于出厂价。〔37〕对这些社区团购平台而言，利用算法设置个性化的超低价格具有很

〔32〕 See OECD, Personalised Pricing in the Digital Era-Note by the European Union, pp. 6－7, DAF/COMP/WD (2018) 128.

〔33〕 参见邹开亮、刘佳明：《大数据“杀熟”的法律规制困境与出路——仅从〈消费者权益保护法〉的角度考量》，载《价格理论与实践》2018年第8期。

〔34〕 参见李成：《人工智能歧视的法律治理》，载《中国法学》2021年第2期。

〔35〕 参见史洪举：《以司法裁判向大数据杀熟说不》，载《人民法院报》2021年7月17日，第02版。

〔36〕 See Ariel Ezrachi, Maurice E. Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Harvard University Press, 2016, pp. 119, 297.

〔37〕 参见吴睿鹏：《警惕社区团购“烧钱大战”戕害市场竞争秩序》，载《中国消费者报》2020年12月15日，第001版。

大的吸引力。

（3）一般价格

除超高价格和超低价格之外的价格，都是一般价格。大部分算法个性化定价都是这种价格。〔38〕正如欧盟 2018 年调研报告所指出的，实践中算法个性化定价的平均价差基本不超过 1%，最大价差也低于 4%。〔39〕这意味着算法个性化定价普遍价差幅度不大，并非明显低于或高于市场价值。由此衍生的相关问题是：一般价格场景下的算法个性化定价是否具有危害性，是否因属于经营者自主定价范围而可采取“自由放任”的态度。

三、一般价格的危害性再审视

超高价格与超低价格的算法个性化定价危害较为明确，而一般价格的危害比较模糊，有必要再审视一般价格场景下算法个性化定价的危害，从而明确是否需要规制以及如何规制。

（一）一般价格危害性的“去伪”

既有研究采用一般化的分析，认为算法个性化定价兼具侵犯消费者权益、剥削消费者剩余以及扭曲市场竞争的危害性。然而，一般价格场景下的算法个性化定价并不具有前述危害。

1. 一般价格的危害不在于损害消费者权益

一般价格场景下算法个性化定价并不具有损害消费者权益的危害性。第一，消费者法定权利未受侵害。不少观点曾主张算法个性化定价损害了消费者知情权和自主选择权，应予禁止。〔40〕然而，这类观点违背了法律条文的通常含义，为学者所批判。〔41〕实际上，《消费者权益保护法》第 8 条规定的知情权，只是知悉商品或服务“真实情况”的权利，不包括经营者与其他消费者的交易价格。经营者与其他主体的交易情况，有时甚至可能构成商业秘密。第 9 条明确了消费者享有自主选择权，“有权进行比较”，但比较的对象是商品，而不是成交价。《消费者权益保护法》第 20 条和《价格法》第 13 条规定的经营者“明码标价”义务，〔42〕只要求经营者明确标示价格，不要求经营者在不同时间针对不同人的报价均保持一致，否则便可能违背《价格法》第 11 条规定的经营者自主定价权。《互联网信息服务算法推荐管理规定》第 21 条从保护公平交易权的角度规制算法个性化定价，这种思路得到了一些学者的认可。但本文认为，公平交易权的规制路径或可适用于超高价格的场景，但在一般价格场景下，经营者并未向消费者收取不公平高价，并未侵

〔38〕 参见施春风：《定价算法在网络交易中的反垄断法律规制》，载《河北法学》2018 年第 11 期。

〔39〕 See European Commission (EC), Consumer Market Study on Online Market Segmentation Through Personalised Pricing/Offers in the European Union, p. 219, June 2018, available at https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/synthesis_report_online_personalisation_study_final_0.pdf, last visited on Jan. 5, 2022.

〔40〕 参见陈兵：《法治经济下规制算法运行面临的挑战与响应》，载《学术论坛》2020 年第 1 期；雷雨田：《运用大数据不宜“看人下菜碟”》，载《经济日报》2021 年 3 月 16 日，第 09 版。《禁止网络不正当竞争行为规定（公开征求意见稿）》也从这一角度提出了应规制算法个性化定价。

〔41〕 参见杨成越、罗先觉：《算法歧视的综合治理初探》，载《科学与社会》2018 年第 4 期。

〔42〕 有观点便认为算法个性化定价违背“明码标价”要求。参见刘佳明：《大数据“杀熟”的定性及其法律规制》，载《湖南农业大学学报（社会科学版）》2020 年第 1 期。

害消费者公平交易权。

第二，消费者剩余并不必然减少。有研究表明，有时算法个性化定价会导致整体福利提高而适度降低个体消费者剩余，有时算法个性化定价会刺激竞争进而有利于消费者。〔43〕一般价格场景对消费者剩余而言兼具积极和消极影响，很难精确判断其具体效果。〔44〕尽管可以确定，若能实现经济学意义上的一级价格歧视，则一定会损害消费者权益，〔45〕但就当下实践与方法而言，尚无证据证明经营者能够实现真正的一级价格歧视。

第三，即便一般价格场景下特定消费者权益一定程度上受损，也无需政府干预。首先，一般价格场景下的算法个性化定价符合商业惯例，在现实生活中是比较常见的。只要不构成欺诈、不公平价格等情形，法律一直采取的是放任态度，任由市场自发调节。其次，消费者可采取措施自我保护。“杀熟”靠技术，“反杀熟”靠智慧。〔46〕通过增加搜索次数、迟延支付等方式将自己包装成谨慎的消费者，消费者大概率可避免被经营者收取相对高价。质疑观点可能会认为这会增加消费者交易成本，但多次搜索不过是消费者自我保护的体现，也是《消费者权益保护法》第13条对消费者的期待。

2. 一般价格的危害性不在于排除限制竞争

一般价格场景下的算法个性化定价危害不在于排除限制竞争，不应由《反垄断法》规制。第一，并未违反《反垄断法》的具体规定。《反垄断法》第17条第1款第6项关于差别待遇的规定，被有的学者认为可用于规制一般价格场景下的算法个性化定价——“没有正当理由，对条件相同的交易相对人在交易价格等交易条件上实行差别待遇”。然而，对该条进行规范分析可以发现，遭受差别待遇的对象是“交易相对人”，其仅指经营者，并不包括终端消费者。首先，参与立法起草审议的立法工作者指出，差别待遇被《反垄断法》禁止的原因在于该行为会“致使有的交易相对方处于不利的竞争地位”〔47〕，这意味着“交易相对人”仅指经营者，而不包括消费者。其次，《反垄断法》第14条关于垄断协议的规定也使用了“交易相对人”的表述，这里的“交易相对人”通常不包括终端消费者。根据一致用法推定的解释原则，词语应被推定在同一法律文本中具有相同的含义，〔48〕那么《反垄断法》第17条第1款第6项规定的“交易相对人”也不应包括终端消费者。最后，反对观点主张采用目的性扩张解释，通过援引目的条款中的“维护消费者利益”将第6项扩张适用于针对终端消费者的差别待遇。也有观点提出可从剥削性滥用的角度规

〔43〕 See Mark Armstrong, Recent Developments in the Economics of Price Discrimination, in Richard Blundell et al. ed., *Advances in Economics and Econometrics: Theory and Applications, Ninth World Congress*, Cambridge University Press, 2013, pp. 114 - 115, 120 - 126.

〔44〕 See Pascale Chapdelaine, Algorithmic Personalized Pricing, 17 *New York University Journal of Law and Business*, 1, 29 (2020); William W. Fisher III, When Should We Permit Differential Pricing of Informatioin? 55 *UCLA Law Review*, 1, 20 - 37 (2008); 王文君：《算法个性化定价的反垄断法反思》，载《甘肃政法大学学报》2021年第5期。

〔45〕 参见方师师：《用大数据方法破解“大数据杀熟”》，载《光明日报》2021年4月30日，第02版。

〔46〕 参见文阳：《“杀熟”靠技术，“反杀熟”靠智慧》，载 https://static.cdsb.com/micropub/Articles/202103/44ea81710cd04a6604253c6b25fb4403.html，最后访问时间：2022年1月5日。

〔47〕 安建主编：《中华人民共和国反垄断法释义》，法律出版社2018年版，第51页。

〔48〕 参见王利明：《法学方法论》，中国人民大学出版社2012年版，第381页；Antonin Scalia, Byran A. Garner, *Reading Law: The Interpretation of Legal Texts*, Thomson/West, 2012, p. 186.

制一般价格场景下的算法个性化定价。〔49〕但如前所述，一般价格场景下的算法个性化定价并不损害消费者权益，援引一般条款或剥削性滥用条款难以成立。

第二，一般价格场景下的算法个性化定价不具有排除限制竞争的实质危害性。直接以终端消费者为客体的差别待遇，一般而言不具有排除限制竞争的效果。〔50〕所谓“排除限制竞争”，是指排除限制企业之间的竞争。一般价格场景下的算法个性化定价显然不具有排除限制竞争效果。

第三，《反垄断法》的内在逻辑也决定了一般价格场景下的算法个性化定价不应由《反垄断法》规制。《反垄断法》的内在逻辑在于恢复市场竞争，使市场机制运行正常，不能也不应该涉足即使是正常市场机制也无法解决的领域。与格式合同附随条款因缺乏关注而易形成垄断均衡一样，〔51〕一般价格场景下的算法个性化定价同样难以被消费者关注，这意味着即使由《反垄断法》调整并恢复至自由竞争市场，也仍然会出现此类算法个性化定价行为。

（二）一般价格危害性的“存真”

一般价格场景下的算法个性化定价不损害消费者利益，也不扭曲市场竞争，是否意味着其不具有危害性？自由主义学派可能会主张一般价格应该得到尊重，因为这是经营者行使自由定价权的必然结果，是市场经济的核心特征。〔52〕例如美国代表及工商业咨询委员会（BIAC）在经济合作与发展组织（OECD）“数字时代的个性化定价”圆桌会上都明确提出若不涉及反竞争效果、不公平或欺诈的行为，算法个性化定价便不构成竞争或消费者权益保护问题，此时应避免过度执法可能带来的问题。〔53〕但与会的英国代表提出，除了竞争与消费者权益保护问题外，算法个性化定价还可能会严重影响消费者对数字经济的信心。〔54〕会前 OECD 秘书处提供的背景材料同样指出：个性化定价的实施是不透明的，存在着减少市场信任的风险，可能抑制消费者在数字市场的参与。〔55〕社会舆论普遍认为算法个性化定价会透支消费者信任，引发信任危机。〔56〕那么一般价格场景下的算法个性化定价是否会损害消费者对数字市场的信任？本文给出的是肯定回答。

1. 消费者信任经营者

数字市场上，消费者对经营者具有实然和应然的信任。首先，“信任”的经典含义是指 A 方愿意将自己软肋暴露给 B 方并期待着 B 方会为 A 方利益行事，而不管 A 方是否有能力对 B 方进

〔49〕 参见郝俊淇：《平台经济领域差别待遇行为的反垄断法分析》，载《法治研究》2021 年第 4 期。

〔50〕 参见丁茂中：《论差别待遇的合理性分析标准》，载《上海对外经贸大学学报》2018 年第 5 期。

〔51〕 参见马辉：《格式条款信息规制论》，载《法学家》2014 年第 4 期；解亘：《格式条款内容规制的规范体系》，载《法学研究》2013 年第 2 期。

〔52〕 参见梁正、曾雄：《“大数据杀熟”的政策应对：行为定性、监管困境与治理出路》，载《科技与法律》2021 年第 2 期。

〔53〕 See OECD, Personalised Pricing in the Digital Era-Note by the United States, DAF/COMP/WD (2018) 140; OECD, Personalised Pricing in the Digital Era-Note by BIAC, DAF/COMP/WD (2018) 123.

〔54〕 See OECD, Personalised Pricing in the Digital Era-Note by the United Kingdom, DAF/COMP/WD (2018) 127.

〔55〕 See OECD, Personalised Pricing in the Digital Era: Background Note by the Secretariat, DAF/COMP (2018) 13.

〔56〕 参见周菊：《大数据“杀熟”是透支消费信任》，载《中华工商时报》2018 年 3 月 2 日，第 003 版；刘丽、郭苏建：《大数据技术带来的社会公平困境及变革》，载《探索与争鸣》2020 年第 12 期。

行监督或控制。〔57〕这一定义已得到普遍认可。〔58〕其次，消费者对经营者的信任，直接体现在消费者依据《网络安全法》和《个人信息保护法》同意向经营者提供可能对消费者不利的信息，同意的结果使得消费者的弱势地位更为明显。这种同意行为意味着消费者信任经营者不会利用这些信息对消费者不利。再次，消费者对具有强大算力的经营者的信任，还体现在消费者对这些类似于“专家系统”的经营者的信任，相信他们发挥着第三方监管的作用。〔59〕最后，从应然层面来看，消费者对经营者的信任是数字经济发展所必然要求的。尤其在网络时代，信任发挥着类似于“公地资源”〔60〕或“数字经济的货币”〔61〕的重要作用。

2. 主观不公平感会减损消费者信任

算法个性化定价会破坏消费者对特定经营者的信任，其内在逻辑在于算法个性化定价会引发消费者主观不公平感，这种不公平感会削弱消费者的信任。

第一，调查问卷清楚表明消费者对算法个性化定价的主观感受。2019 年北京市消协发布相关调查报告，数据显示有 82.54％的被调查者认为算法个性化定价将严重透支消费者信任、降低企业声誉，81.41％的被调查者认为算法个性化定价会损害消费者权益。〔62〕2020 年南都反垄断研究课题组发布的《互联网平台竞争与垄断观察报告》显示，1300 多名受访者中有 73％反对算法个性化定价。〔63〕此外，有学者在调查美国 1500 户家庭后发现，约有 91％的受访者对算法个性化定价表示强烈反感，87％的受访者认为这种行为是错误的，76％的受访者会因为他人支付相对低价而懊恼。〔64〕一项针对近 300 名学生的调研显示，受访者倾向于认为算法个性化定价严重影响消费者对公平的感知。〔65〕另一项调研显示，78％的消费者甚至不希望得到基于上网痕迹提供的个性化折扣。〔66〕在对荷兰上千位消费者进行问卷调查后，有研究发现超过 80％的消费者认为算法个性化定价是不公平的、不可接受的，应予禁止。〔67〕欧盟委员会 2018 年进行的针对 2 万

〔57〕 See Roger C. Mayer, James H. Davis, F. David Schoorman, An Integrative Model of Organizational Trust, 20 *The Academy of Management Review*, 709, 712 (1995).

〔58〕 See Ellen Garbarino, Olivia F. Lee, Dynamic Pricing in Internet Retail: Effects on Consumer Trust, 20 *Psychology and Marketing*, 495, 500 (2003).

〔59〕 参见李飞翔：《“大数据杀熟”背后的伦理审思、治理与启示》，载《东北大学学报（社会科学版）》2020 年第 1 期。

〔60〕 谢尧雯：《网络平台差别化定价的规制路径选择——以数字信任维系为核心》，载《行政法学研究》2021 年第 5 期，第 27－28 页。

〔61〕 许可：《数字经济视野中的欧盟〈一般数据保护条例〉》，载《财经法学》2018 年第 6 期，第 74 页。

〔62〕 参见前引〔9〕。

〔63〕 参见黄莉玲、李玲、黄慧诗：《南都发布〈互联网平台竞争与垄断观察报告〉市场竞争失序产生垄断要大力监管》，载《南方都市报》2020 年 12 月 23 日，第 A07 版。

〔64〕 See Joseph Turrow, Lauren Feldman, Kimberly Meltzer, Open to Exploitation: America's Shoppers Online and Offline, A Report Annenberg Public Policy Center of the University of Pennsylvania, June 2005, available at https://repository.upenn.edu/asc_papers/35, last visited on Jan. 5, 2022.

〔65〕 See Kelly L. Haws, William Bearden, Dynamic Pricing and Consumer Fairness Perceptions, 33 *Journal of Consumer Research*, 304, 309 (2006).

〔66〕 See Joseph Turrow, Jennifer King, Chris J. Hoofnatle, Amy Bleakley, Michael Hennessy, Americans Reject Tailored Advertising and Three Activities That Enable It, Sept. 29, 2009, available at https://ssrn.com/abstract＝1478214, last visited on Jan. 5, 2022.

〔67〕 See Joost Poort, Frederik Zuiderveen Borgesius, Does Everyone Have a Price? Understanding People's Attitude Towards Online and Offline Price Discrimination, 8 *Internet Policy Review*, 1, 2 (2019).

多消费者的调查结果同样证实了这一结论。〔68〕

综上，算法个性化定价容易引起消费者反感，让消费者感受到不公平。那么，消费者的不公平感从何而来？实际上，差异化价格并非新奇之事，为何有些差异化定价能被消费者接受，而算法个性化定价却会让人感到不公平？下述理论分析能够提供答案。

第二，消费者的不公平感主要源于分配不公平和程序不公平。传统上被消费者接受的差异化价格，大体可分为七种类型。〔69〕这些特殊类型的价格差异能被社会接受的原因主要包括：一是存在被社会习惯所认可和接受的实质正当理由，典例就是学生优惠票或飞机票价的动态变化，如郑某诉携程案涉及的就是机票动态变化。〔70〕二是定价政策公开、透明，消费者要么能够参与定价过程，要么有更多自由选择的空间，此时消费者更容易认可价格差异，典例如量多优惠。

前述理由，有助于反向理解为何算法个性化定价被消费者认为是不公平的。算法个性化定价引致的消费者不公平感可分为两类：分配不公平（distributive unfairness）和程序不公平（procedural unfairness）。〔71〕首先，算法个性化定价违背了分配公平却无正当理由。一般价格场景下的算法个性化定价呈现出“千人千价”“最懂你的人伤你最深”的特点。而且通常而言，算法个性化定价总是对“熟人”收取更高价格，这违背了“人熟为宝”的传统商业道德。〔72〕其次，算法个性化定价透明度低且没有退出机制，违背了程序公平。消费者无法了解自己是否被个性化定价，也不清楚个性化定价的机制，甚至没有办法选择退出个性化定价，这会加剧消费者的不公平感，损害消费者信任。〔73〕

第三，质疑观点可能会主张如果算法个性化设定的价格是一般价格，此时因为消费者自愿同意接受该价格，再加上经营者也没有实施欺诈行为，所以应该认定价格是公平的。这是传统定价理论对公平价格的理解，即商品的公平价格是购买者在真空状态下的独立判断。但行为经济学指出，消费者具有从众心理，他们对商品价值的判断大多是基于他人支付的价格。换言之，公平价格的判断并非消费者在真空状态下的独立判断。当消费者意识到他人支付的价格更低时，消费者便会认为自己所支付的价格并非公平价格。理查德·塞勒提出的“交易效用”（transaction utility）理论可以很好地解释为什么消费者会认为一般价格场景下算法个性化定价是不公平的。

---

〔68〕 See EC, Consumer market study on online market segmentation through personalised pricing/offers in the European Union, June 2018, available at https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/synthesis_report_online_personalisation_study_final_0.pdf, last visited on Jan. 5, 2022.

〔69〕 一是基于特定身份群体的折扣价，比如老人、学生、儿童；二是基于数量的折扣价，也就是所谓的量多优惠；三是忠诚折扣，即重复多次购买而可以享受熟人优惠；四是新客折扣，这在双边平台市场的合理性更为明显；五是根据使用峰值、谷值与平值而差异定价，常见的如分时电价；六是基于时间的折扣，比如飞机票价的优惠；七是基于消费者讨价还价能力而形成的差异价格。

〔70〕 参见上海市第一中级人民法院（2020）沪 01 民终 13989 号民事判决书。

〔71〕 See Jennifer Lyn Cox, Can differential prices be fair? 10 *Journal of Product & Brand Management*, 264, 265－267 (2001).

〔72〕 参见杨燕明：《“数据杀熟”：刹住技术歪心思》，载《人民法院报》2020 年 9 月 19 日，第 002 版。

〔73〕 See Mariateresa Maggiolino, Personalized Prices in European Competition Law, Jun. 12, 2017, Bocconi Legal Studies Research Paper No. 2984840, available at https://ssrn.com/abstract=2984840, last visited on Jan. 5, 2022.

因为交易效用取决于商品成交价与参考价之间的差别，当消费者以他人的成交价为参考价而发现自己成交价更高时，交易效用将受损，不公平感油然而生。〔74〕需要注意的是，信任是观念层面的概念，信任的损害不要求是实际损害，只要消费者主观感受到价格不公平即可。〔75〕

3. 消费者信任受损的危害性

一般价格场景下的算法个性化定价尽管并不会损害消费者权益，也不会扭曲市场竞争，但会导致消费者对特定经营者的信任受损，进而会产生如下危害：

第一，算法个性化定价会使消费者对整个数字经济的信任度下降。例如原英国公平交易局（OFT）在2013年的报告中提出，算法个性化定价会降低消费者对网络交易市场的信任。〔76〕在OECD“数字时代的个性化定价”圆桌会议中，英国CMA进一步阐述了个性化定价对消费者信任以及数字经济发展的影响：“消费者信任的缺乏不仅与实施个性化定价的企业相关，而且还与整个网络经济有关。”〔77〕2021年CMA再次强调消费者对网络市场的信任会遭受损害从而损害整体经济效率。〔78〕消费者对特定经营者的不信任会波及整个数字市场，一方面是因为消费者认为算法个性化定价在数字经济时代较为普遍，〔79〕另一方面也因为算法个性化定价的行为主体、〔80〕影响程度和波及范围具有普遍性。总而言之，针对单个经营者的不信任会波及整个网络市场。〔81〕

第二，消费者信任受损会破坏市场秩序，阻碍网络经济蓬勃发展。具体到我国近期的国家政策，这还可能会影响国内、国际双循环的构建，影响到新产品和新科技的更新换代。行为经济学发现，消费者具有损失厌恶的特征，会避免陷入使他们后悔的交易中。可以预见的是，具有损失厌恶特征的消费者在信任受损后将更谨小慎微，更不愿意参与到网络交易中。〔82〕行为经济学的实证研究也证实了消费者在感受到不公平后会结束交易。〔83〕信任受损之后，消费者将会减少他们的需求，最终会损害消费者剩余。〔84〕总而言之，消费者信任受损会冲击网络经济市

〔74〕 See Richard H. Thaler, Mental Accounting and Consumer Choice, 4 *Marketing Science*, 199 (1985).

〔75〕 See Ellen Garbarino, Olivia F. Lee, Dynamic Pricing in Internet Retail: Effects on Consumer Trust, 20 *Psychology and Marketing*, 495, 500 (2003).

〔76〕 See UK Office of Fair Trading (OFT), Personalized Pricing: Increasing Transparency to Improve Trust, OFT 1489, May 2013, available at https://webarchive.nationalarchives.gov.uk/20140402165101/http://oft.gov.uk/shared_oft/markets-work/personalised-pricing/oft1489.pdf, last visited on Jan. 5, 2022.

〔77〕 OECD, Personalised Pricing in the Digital Era-Note by the United Kingdom, pp. 9 - 10, DAF/COMP/WD (2018) 127.

〔78〕 参见前引〔12〕，CMA文，第8页。

〔79〕 例如北京消协超过3000份的调查问卷结果显示88.32%的被调查者认为算法个性化定价很普遍。参见前引〔9〕。

〔80〕 普通公司也可实现算法个性化定价。See Micheal Levine, Price Discrimination Without Market Power, 19 *Yale Journal on Regulation*, 1 (2002).

〔81〕 See The National Association of Citizens Advice Bureaux, A price of one's own-an investigation into personalized pricing in essential markets, pp. 18 - 19, available at https://www.citizensadvice.org.uk/Global/CitizensAdvice/Consumer%20publications/Personalised%20Pricing%20Report%202018.pdf, last visited on Jan. 5, 2022.

〔82〕 See Andrew M. Odlyzko, Privacy, Economics, and Price Discrimination on the Internet, International Conference on Electronic Commerce, Jul. 27, 2003, available at https://ssrn.com/abstract=429762, last visited on Jan. 5, 2022.

〔83〕 See Domen Malc, Damijan Mumel, Aleksandra Pisnik, Exploring Price Fairness Perceptions and Their Influence on Consumer Behavior, 69 *Journal of Business Research*, 3693 (2016).

〔84〕 See OFT, The Economics of Online Personalised Pricing, pp. 83 - 87, May 2013, available at https://webarchive.nationalarchives.gov.uk/20140402154756/http:/oft.gov.uk/shared_oft/research/oft1488.pdf, last visited on Jan. 5, 2022.

场秩序。

综上，基于危害差异及概念逻辑，本文将算法个性化定价分为三个非空子类：超高价格、超低价格、一般价格。

四、规制算法个性化定价的策略

本部分将围绕各类算法个性化定价的危害及其损害机理提出具体规制进路。

（一）危害性的识别方法

在提出具体规制进路之前，有必要先解决如何识别不同种类的算法个性化定价这一实践难题。算法个性化定价的理论分类是方便且容易的，但因算法行为具有隐蔽性特征且难以从外部对其进行观察，所以要识别具有不同危害性的行为在实践中并非易事。尽管如此，我们仍然可以运用区块链技术可溯源与可追踪的特点，从数据输入、代码计算与算法输出三个层面来识别危害性。

识别算法个性化定价与算法合谋定价、欺诈定价、歧视定价，首先，可以通过直接访问数据和代码来分辨不同的损害。直接访问数据和代码有助于监管者更精确地认知算法逻辑，做出更有效的监管。比如某些情况下，数据本身就能表明是否存在种族与性别歧视问题。但直接访问数据和代码需要公司的高度配合，这需要考虑公司的激励问题，以及政府干预的限度问题。其次，在无法直接访问数据和代码时，可以从数据输入和算法输出两个角度来间接了解算法的运作机制。一般而言可以通过“抓取审核”（scraping audit）的方式或通过应用程序接口（API）来识别不同的危害性。最后，在没有现实数据时还可以采用创建虚拟角色测试的方式，如欧盟 2018 年、北京消协 2019 年都曾采用此种调研方法。

识别算法个性化定价的三种子类行为无涉算法，这是因为价格的高低只是算法输出的结果，不需要深入算法内部即可从外部观察并区分这三种子类行为。算法个性化定价子类行为的判断标准，与线下世界对超高价格、超低价格、一般价格的判断标准是类似的。超高价格的判断可以借鉴反垄断法关于超高价格的判断标准，〔85〕也可以借鉴合同法关于显失公平客观要件的判断标准，甚至还可以借鉴《最高人民法院关于适用〈中华人民共和国合同法〉若干问题的解释（二）》第 19 条关于 30％价差的相关规定。超低价格判断因素与超高价格的判断因素类似，可以从《价格法》《反垄断法》相关的规定中汲取相应的考虑因素，例如判断定价是否低于平均可变成本，另外 30％的价差或可以作为参考因素。

（二）基于危害性差异的分类规制

1. 超高价格和超低价格的规制路径

超高价格与超低价格具有严重危害，因此法律基本持禁止态度。

〔85〕 参见梅夏英、任力：《关于反垄断法上不公平高价制度的法律适用问题》，载《河北法学》2017 年第 4 期；苏华：《不公平定价反垄断规制的核心问题——以高通案为视角》，载《中国价格监管与反垄断》2014 年第 8 期。

第一，超高价格的危害性在于剥夺消费者剩余，损害公平交易，可适用《反垄断法》第17条第1款第1项、《民法典》第151条、《互联网信息服务算法推荐管理规定》第21条或《消费者权益保护法》第10条和第16条予以规制。具体来说，若经营者具有市场支配地位，利用消费者画像收取超高价格，则可能违反《反垄断法》关于不公平高价的规定。当经营者不具有市场支配地位时，则可以适用《民法典》第151条调整经营者利用消费者处于危困状态、缺乏判断能力等情形设定超高价格致使显失公平的行为。《消费者权益保护法》第10条规定了消费者有权获得价格合理的公平交易条件，第16条要求经营者承担不得设定不公平交易条件的义务。《互联网信息服务算法推荐管理规定》第21条同样是基于消费者的公平交易权介入规制。

第二，超低价格的危害性在于扰乱市场竞争秩序，在经营者处于市场支配地位时还会产生排除限制竞争的效果，可通过《反垄断法》和《价格法》进行调整。当经营者具有市场支配地位时，若算法个性化定价属于超低价格，低于平均可变成本，便可能会违反《反垄断法》第17条第1款第2项而构成掠夺性低价。若不具有市场支配地位，经营者利用算法设定超低价格的行为仍然可能违反《价格法》第14条之规定。2021年7月国家市场监督管理总局发布的《价格违法行为行政处罚规定（修订征求意见稿）》提高了这一新型价格违法行为的罚款力度，相信能够有效应对其危害性。

第三，超高价格和超低价格的危害性还可以通过事前规制的方法予以调整。比如可以设定价格区间限制（price caps），即利用算法设定的个性化价格应保持在合理的区间范围。英国金融行为监管局（Financial Conduct Authority）曾采用这种方式。〔86〕这种规制方法具有一定的正当性，得到了学者的支持。〔87〕

2. 一般价格的多元共治路径

政府原则上不应介入规制一般价格场景下的算法个性化定价，因为市场机制会逼迫经营者进行竞争从而实现竞争均衡，而且即便在垄断性市场上利用算法设定一般价格也不会损害消费者权益，不会扭曲市场竞争。不过算法个性化定价可能会弱化消费者信任、破坏市场秩序，此时政府需要介入规制以重建市场信任。而重建市场信任是个系统工程，需要政府、经营者与消费者共同努力，形成多元共治的规制格局。

（1）一般价格场景的政府介入规制路径

为维系消费者对经营者及数字经济的信任，政府应介入调整一般价格场景下的算法个性化定价行为，需要注意如下三点：

第一，坚持包容审慎的监管原则，具体包括依法监管、科学监管、积极有效监管等内涵。首

〔86〕 See Financial Conduct Authority, Price Discrimination in Financial Services: How Should We Deal With Questions of Fairness? p. 9, July 2018, available at: https://www.fca.org.uk/publication/research/price_discrimination_in_financial_services.pdf, last visited on Jan. 5, 2022.

〔87〕 See Oren Bar-Gill, Algorithmic Price Discrimination When Demand is a Function of Both Preferences and (Mis) perceptions, 86 *University of Chicago Law Review*, 217, 243 (2019).

先应尽可能减少对市场的干预，充分发挥市场的调节作用。市场可能会自发催生比价网站，通过算法技术帮助消费者反“杀熟”。〔88〕其次，政府要灵活运用多种规制工具重建消费者对数字经济的信任，例如可以通过行政指导等软性规制方法强化对算法个性化定价的监管。〔89〕最后，包容审慎监管并不意味着不监管和弱监管，因为消费者信任类似于“公地资源”，若不施加干预可能会出现“数字信任公地悲剧”。〔90〕

第二，政府应围绕信任损害机制重建信任，主要可以从维护程序公平的角度设计具体监管方法。首先，政府可以要求经营者提高数据与算法的透明度，从而维护消费者对数字市场的信任。设定经营者强制告知规则是提高透明度的有效方案，〔91〕例如可以在个人数据保护规范中强制要求经营者告知算法个性化定价的基本原理和主要运行机制〔92〕。需要注意的是，提高透明度的同时务必要提防经营者通过共享用户个性化数据而实现算法共谋。〔93〕其次，政府可强制要求经营者为消费者提供便利的退出机制。如果能为消费者提供更方便的退出机制，他们将对算法个性化定价持更为积极的态度。〔94〕我国《互联网信息服务算法推荐管理规定》第 16 条和第 17 条强调了强制告知和退出机制的作用，美国众议院立法小组 2021 年 6 月提出的《过滤气泡透明度法案》(Filter Bubble Transparency Act) 以及欧洲议会最新通过的《数字服务法》亦强调透明度和退出机制的重要性。

第三，政府应加强消费者教育，让消费者正确认识算法个性化定价。当前消费者对算法个性化定价的认知仍停留在感性层面，普遍认为算法个性化定价就是“杀熟”。在这种感性的认知下，消费者信任很难建立。推动消费者理性看待算法个性化定价是政府维系数字经济信任的重要环节。政府可以通过公开市场调研报告等手段增强消费者的信任，或者可基于信任机制重构算法解释权，使算法个性化定价更能得到接受与认可。〔95〕

(2) 一般价格场景的经营者自我规制路径

消费者信任是经营者的一种商誉，对经营者的经营活动具有重要价值，因此经营者也应该强化自我规制。从实际效果来看，经营者自我规制也是治理算法个性化定价诱致信任危机最为便捷的方式。经营者可从如下三个方面调整经营行为：

第一，从矫正程序公平的角度而言，经营者不仅要提高算法个性化定价的透明度，还要主动

〔88〕 参见乔榛、刘瑞峰：《大数据算法的价格歧视问题》，载《社会科学研究》2020 年第 5 期。

〔89〕 参见《盒马、京东等 10 平台签署承诺书：不利用大数据“杀熟”》，载 http://news.winshang.com/html/068/3405.html，最后访问时间：2022 年 1 月 5 日。

〔90〕 参见前引〔60〕，谢尧雯文。

〔91〕 英国议会上议院在 2016 年也曾建议政府采取这种强制告知规则。See House of Lord, Online Platforms and the Digital Single Market, p. 76, Apr. 20, 2016, available at https://publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/129.pdf, last visited on Jan. 5, 2022.

〔92〕 See Frederik Zuiderveen Borgesius, Joost Poort, Online Price Discrimination and EU Data Privacy Law, 40 *Journal of Consumer Policy*, 347, 358 - 360 (2017).

〔93〕 See Terrell McSweeny, Brian O'Dea, The Implications of Algorithmic Pricing for Coordinated Effects Analysis and Price Discrimination Markets in Antitrust Enforcement, 32 *Antitrust*, 75 (2017).

〔94〕 See Gerhard Wagner, Horst Eidenmüller, Down by Algorithms: Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions, 86 *University of Chicago Law Review*, 581, 592 (2019).

〔95〕 参见丁晓东：《基于信任的自动化决策：算法解释权的原理反思与制度重构》，载《中国法学》2022 年第 1 期。

为消费者提供更为便利的退出机制。经营者还可以设计流程让消费者切身参与到个性化定价过程中，减少其程序不公平感。〔96〕第二，从矫正分配公平的角度而言，经营者可以告知消费者个性化定价的正当理由，减少消费者的不公平感。例如在网约车场景下，平台提供个性化的配车服务或加速配车服务可以主动告知消费者为此需要提高价格，这种情形下的差异化定价更容易让消费者接受。同时，经营者还可以从折扣和优惠的角度表述算法个性化定价，提高消费者的接受度。第三，经营者可通过减少交易的相似性减轻消费者的不公平感。〔97〕消费者是通过比对相似交易下其他消费者支付的价格而获得不公平感的，那么在差异化经营模式下，消费者不公平感会逐渐减少。

（3）一般价格场景的消费者自我保护路径

数字经济是未来经济发展的方向，会给消费者带来许多意想不到的益处。算法个性化定价会给消费者带来便利，有时也能提高消费者剩余。我们不能一味强调消费者的弱势地位并要求政府和经营者给予帮助和保护，实际上消费者也可以在算法个性化定价的治理体系中发挥重要作用。从消费者角度来看，重建市场信任需要消费者努力做到以下两个方面：第一，消费者应更理性地看待算法个性化定价。算法个性化定价形成的超高价格和超低价格确实会损害消费者权益，但并非所有的算法个性化定价都会如此。一般价格场景下的算法个性化定价并未侵害消费者权益，因此消费者不应将所有算法个性化定价同等对待。第二，消费者应提高自我保护意识，在交易时应更为慎重，尽量减少对单一软件的依赖，同时还可以通过多次搜索浏览比价以强化自我保护。尽管要求经营者自我规制是更直接的解决路径，但多举措齐头并进才能实现更好的规制。对消费者个体而言，提高自我保护意识能屏蔽掉多数风险。此外，还可以通过算法赋能消费者，用大数据方法来破解算法个性化定价。〔98〕

五、结　论

规制算法个性化定价应遵循对策与问题相匹配的规制法原理，不仅要将算法个性化定价与诸如算法欺诈定价、歧视定价、合谋定价等其他算法危害行为区分开，避免混淆，还要根据危害差异将算法个性化定价进行细分（超高价格、超低价格和一般价格）。超高价格和超低价格场景下的算法个性化定价可通过《反垄断法》《民法典》《价格法》和《消费者权益保护法》等法律事后规制，也可通过设定价格区间限制进行事前调整。一般价格场景下的算法个性化定价之危害性既不在于损害消费者权益，也不在于排除限制竞争，而在于让消费者产生价格不公平的感受，进而削弱消费者信任，放任其发展甚至可能会破坏市场秩序。基于维系消费者信任、重建市场信心的

〔96〕 See Timothy J. Richards, Jura Liaukonyte, Nadia A. Streletskaya, Personalized Pricing and Price Fairness, 44 *International Journal of Industrial Organization*, 138 (2016).

〔97〕 See Lan Xia, Kent Monroe, Jennifer Cox, The Price is Unfair! A Conceptual Framework of Price Unfairness Perceptions, 68 *Journal of Marketing*, 1, 8 (2004).

〔98〕 See Michal S. Gal, Niva Elkin-Koren, Algorithmic Consumers, 30 *Harvard Journal of Law & Technology*, 309, 310 (2017).

需要，政府、经营者和消费者应合力推动一般价格场景下算法个性化定价的治理：政府应坚持包容审慎监管，强制经营者履行告知义务，强制经营者建立消费者自由退出机制；经营者要紧抓消费者信任的损害机理，围绕分配公平和程序公平两个层次调整经营行为；消费者则要理性对待、提高警惕，利用自己的智慧反“杀熟”。

Abstract：The regulatory practices and theoretical analysis of algorithm personalized pricing fail to follow the regulatory principle of matching regulation countermeasures with the hazards. According to the principle, we should pay attention to the differences between algorithm personalized pricing and algorithm collusion pricing, fraudulent pricing, discriminatory pricing, personalized recommendation. Meanwhile, the complexity of hazards requires us to deconstruct the algorithm personalized pricing into three subcategories: ultra-high price, ultra-low price and ordinary price. The hazards of ultra-high and ultra-low price scenarios can be resolved under the existing legal framework. In ordinary price scenario, algorithm personalized pricing will not infringe consumers' rights and interests, nor eliminate and restrict competition. However, it will damage consumers' trust and disorder the digital market from the perspective of distributive unfairness and procedural unfairness. The government, business operators and consumers should work together to establish consumers' trust, based on the understanding and use of the damage mechanism of consumers' trust, so as to achieve a dynamic balance between innovative development and consumer interests protection.

Key Words：big data kill, algorithm personalized pricing, typological analysis, consumers' trust

（责任编辑：李　敏　赵建蕊）

财经法学 No. 3，2022
pp. 16 - 28

公共决策算法的程序规范
——以立法性算法为例

刘佳明*

内容提要：立法性算法是有权机关依照一定程序使用的、能够对公民权利义务产生实质性影响的公共决策算法。与传统立法一样，立法性算法会改变社会资源的分配格局以及人们行为的活动空间，甚至能对公民的权利和义务产生实质性影响。但是，立法性算法所固有的技术性特征，规避了公众对立法性算法程序设计的参与和监督。一方面，构成立法性算法的人工语言与普通公众熟知的自然语言之间存在巨大鸿沟，普通公众因不具备人工语言相关基础知识，难以在算法程序设计中与之进行平等对话和有效沟通，从而使得作为民主性补充渠道的公众参与难以有效进行，进而可能引发监督失效、权责失衡的问题。另一方面，立法性算法会不自觉地嵌入设计者的个人偏好和价值判断，它并不能完全展现“技术中立”理想下的客观和真实，甚至还会出现偏差，从而可能引发算法寻租和算法滥用的问题。要克服立法性算法的缺陷，就要求算法程序的设计必须以透明度和问责制为主要原则，确保公众对立法性算法的充分参与和必要的权利救济途径。

关键词：立法　算法　立法程序　立法性算法　公共决策算法

在法学领域，有关算法的研究主要聚焦于讨论算法与法律之间的内在关系。或是将算法视为法律，认为人类正逐渐成为算法统治的客体；[1] 或是将法律视为算法，认为法律职业者面临即将被算法所取代的危机；[2] 或是认为算法和法律二者是协同共生的关系，寻求用算法推动法律、用法律规训算法的双向规范策略[3]。也许“算法即法律”在当前还言过其实，[4] 但是，不可否认，

* 刘佳明，南京大学法学院博士研究生。

〔1〕 又称“算法法律化”，即人类正逐渐进入算法统治的时代。参见郑戈：《算法的法律与法律的算法》，载《中国法律评论》2018 年第 2 期。

〔2〕 也称“法律算法化”，即法律职业者的推理和判断在多大程度上能够被算法所取代，或者说，法律在多大程度上能够被算法所取代。参见胡凌：《人工智能的法律想象》，载《文化纵横》2017 年第 2 期。

〔3〕 算法和法律二者是协同、共生的关系，即算法和法律相互影响。参见马长山：《智慧社会的治理难题及其消解》，载《求是学刊》2019 年第 5 期。

〔4〕 参见陈景辉：《人工智能的法律挑战：应该从哪里开始?》，载《比较法研究》2018 年第 5 期。

无论在私人领域还是公共领域，人类越来越依赖于算法来进行相关决策。通过将大数据分析和预测技术相结合，算法主体透过算法技术有能力增强其对公民的影响力甚至控制力，从而能够在事实上扩张自身的权力，并实质性影响到公民的权利义务关系，因而必须通过法律对此进行有效规制。〔5〕但是，当前对公共决策领域中算法的规制未能深入系统内部的运行逻辑，导致权力主体对通过程序执行法律的背后行动理由未能提供合理论据和说明，因而也就难以有效应对可能出现的算法寻租和算法滥用问题。对此，应当将公共决策领域中的一部分算法视为立法性算法，从而将立法的民主化和科学化价值导向渗透到算法程序的设计之中，并通过信息公开、公众参与和专家辅助等制度，以民主机制和正当程序保护对算法程序设计的共同体进行持续有效的监控、质询和改造，从而促进立法性算法“黑箱”的程序性净化。

一、何为立法性算法

（一）何为算法

目前学界关于何为“算法”尚未达成共识，有关算法的概念在计算机科学、数学和人文社科等领域不尽相同，试图为算法寻找一个能够涵盖所有领域的概念十分困难。在计算机科学领域，算法被看作是用某种方法解决问题的策略机制，它被具体化为一组准确且完整的描述或一系列清晰的指令。在数学领域，算法则通常被用来描述解决某一问题的操作步骤，它们可以通过数字符号、算盘、图表和计算工具等来执行。〔6〕人文社科中所讨论的算法主要是决策算法，“即在特定情况下所采取的最佳行动，对数据进行最佳解释的算法，这些算法能否增强或取代人类的分析和决策，通常取决于数据和规则的范围或规模”〔7〕。一般而言，针对任何可用于计算的程序操作或决策过程，都可以归入算法的认识范畴，但是，这并不意味着所有与算法有关的问题都可以被纳入公众的讨论范围。事实上，人们对那些公共利益遭受损害，并有可能引发权利义务冲突的算法决策更为关心。在法学领域，人们的关注点聚焦于算法决策的不确定性和不透明性，前者是指基于算法所作出的决策难为他人预测，后者则是指通过算法形成决策所依赖的实质理由和价值取舍难为他人所知。这种算法决策被形象地称为算法“黑箱”。这意味着那些受自动化算法影响的人无法确定决策是如何产生的，也无法对决策背后的因果关系进行逻辑和推理解释，公众因而也就丧失了对其问责的可能。

从实践来看，算法作为一种特殊的决策机制，同时也被视为一种用于建构社会秩序理想模型的方式。在公共政策与公共治理中，权力主体能够借助算法实现政策制定与治理过程的动态化、精细化，从而影响社会主体之间的利益分配关系。〔8〕一方面，以大数据分析和预测技术为基础

〔5〕 参见周辉：《算法权力及其规制》，载《法制与社会发展》2019年第6期。

〔6〕 参见〔美〕瑟格·阿比特博、吉尔·多维克：《算法小时代：从数学到生活的历变》，任轶译，人民邮电出版社2017年版，第6页。

〔7〕 孙保学：《人工智能算法伦理及其风险》，载《哲学动态》2019年第10期，第94页。

〔8〕 参见前引〔5〕，周辉文。

的自动化算法被广泛用于社会治理领域，从而产生大量为受监管实体量身定制的决策或指令，这些决策或指令影响和塑造着不同的社会主体。另一方面，在算法治理之下，这些决策和指令能够参与选择、决定与我们生活相关的各类信息，并最终发展成为管理、判断、调节，甚至能够限制或约束人们行动和生活的强大实体，在客观上也就具有权力属性。〔9〕因此，就公共领域中的某些决策算法而言，其与传统立法在调整社会关系与分配社会利益上具有同质性，即二者都向社会主体提供行为规范，都能改变社会主体之间既有的利益分配格局和行为活动空间，甚至还能对其权利义务产生实质性影响。〔10〕例如，在公共政策制定与社会治理领域，包括经济政策的精准预测和分析，民生管理的精准调度和服务以及公共场所日益增长的自动化监控，这些算法的使用都会涉及立法的内容。

（二）立法性算法的基本内涵

算法与立法既存在共性，也存在一定的差异性。根据算法主体的不同，可以将其划分为公权力算法和私权力算法。前者是指公权力机关所运用的算法，后者一般是指平台企业、数据服务公司等私人主体所运用的算法。而“公权力算法”根据程序性标准又可以划分为“立法性算法”和“非立法性算法”。立法性算法是指有权机关依照一定程序运用的，能够对公民的权利义务产生实质性影响的公共决策算法。例如在疫情防控期间，各地使用的健康码，其背后使用的算法就是严格依照国务院有关部门制定的《个人健康信息码》系列国家标准所形成，这些算法能够根据获取的数据信息自动作出决策对公民行为进行规范和调整，甚至还能对公民的权利义务关系产生实质性影响，如影响公民的消费、出行、工作、生活等。而非立法性算法则是指非经特定程序运用的，但同样能够对公民的权利义务产生实质性影响的公共决策算法。例如“文明码”作为健康码功能的延伸已经从防疫扩展至医疗、养老等其他民生领域，它采用积分模式来对公民的权利义务产生实质性影响，但是，该算法缺乏明确的法律授权，或没有依照特定的立法程序产生，因此，该算法属于非立法性算法。此外，包括公共领域中广泛运用的人脸识别监控算法、社会信用评分算法、智能辅助公共决策算法等，这些算法的使用范围都有可能涉及公民的实质性权利义务，但由于其产生过程未严格依照立法程序进行，因而属于非立法性的算法。因为立法性算法和非立法性算法以其产生过程是否受到立法程序的约束为标准而进行划分，〔11〕所以对立法性算法的产生过程进行程序性规范也就显得尤为重要。事实上，公共决策领域中广泛存在的算法是立法性算法，但算法固有的技术特征规避了立法程序对算法设计的监督和约束作用，从而导致大量立法性算法以非立法性形式在社会治理领域呈现。但是，立法是一种带有价值判断和利益取向的行为秩序安排活动，要使法更好地符合社会需求，就必须通过立法程

〔9〕 关于“算法作为一种权力”的观点最早是由大卫·比尔（David Beer）提出，他认为算法能对每个人施加控制力和影响力，在客观上也是作为一种权力形态而存在。See David Beer, Power through the Algorithm? Participatory Web Cultures and the Technological Unconscious, 11 *New Media & Society*, 985 (2009).

〔10〕 参见蒋舸：《作为算法的法律》，载《清华法学》2019 年第 1 期。

〔11〕 本文将立法视为是一种对不同群体之间利益矛盾和权利冲突进行化解和协调的行为秩序安排。如果用以表示此行为秩序安排的形式是规则化的法律语言，那么此立法就是成文法。如果是裁判，则是判例法。而如果它的表达形式是算法，那么就是立法性算法。

序将不同利益主体的认识纳入评判立法质量的标准体系之中。〔12〕

人们之所以需要法律，是因为人类社会归根结底是一个由各种利益关系交织在一起的复杂体，法律对社会关系的调整实质上也是对社会利益的调整，而权利义务或权力责任等法律概念只是社会主体利益需求在法律上的具体表现形式。“利益作为客观范畴，对法律起着决定性的作用。”〔13〕而人们之所以需要以立法的形式来制定法律，是因为立法作为一种创制权，它以对权力和权利为代表的利益进行分配为目标，立法能够以其公开和透明的程序让普通民众参与其中，并通过合理的整合机制使不同利益群体得以和谐相处。〔14〕因此，立法过程也就是不同社会主体利益需求的表达和博弈过程。〔15〕以司法部 2020 年 2 月 27 日发布的《外国人永久居留管理条例（征求意见稿）》为例，该条例自公布以来就引发了社会各界的高度关注，它的本意是通过赋予外国人永久居留资格来吸引国外人才参与本国建设，从而促进国内经济社会发展。但是，该条例所规定之内容存在诸多不足，导致其自公布以来就受到社会舆论的关注。所幸《中华人民共和国立法法》（以下简称《立法法》）第 67 条专门规定行政法规的起草过程应当向社会公布，并广泛听取公众意见。因为将立法公之于众，无疑会对立法者的选择和决断产生一种无形的压力，从而促使立法活动能够更充分地吸纳并听取公众意见。如果不对立法性算法的产生进行类似规范，这些问题将会同样出现。

而公权力机关之所以需要借助算法的形式实施社会管理，也主要是因为算法对优化治理流程、改善治理精准度以及提升治理效能具有明显的帮助作用。〔16〕然而，在算法治理过程中，看似理性的算法却会引发一系列的算法危机，“算法歧视”“算法合谋”“算法黑箱”等问题层出不穷。〔17〕因为随着社会数字化程度的提高，每个人的生活细节将变得越来越数据化，政府收集和处理数据的算法系统会对公民权利义务产生实质性影响。数据作为算法的根基，决定着算法的目标和实现路径。与此同时，算法也可以被简化为以数据和假设为基础的归纳过程。然而，数据的缺失和预设条件的不合理将直接影响算法的输出结果。当不同决策参数的权重不是由公众参与选择，而是基于特定主体的个人判断之时，算法总是会存在某种程度的不可预测性。即使公众能够直接亲历算法程序设计的全过程，由于对每一个算法程序设计参数缺乏必要的理解，普通民众也将很难做出有效的选择。事实上，在智慧城市建设中，“以支持政府决策和治理为名的大数据中心建设虽然如火如荼，但以算法形式改善决策和治理的成功案例却十分稀少”〔18〕。因为算法程序的设计过程是封闭的，普通公众难以参与到立法性算法程序的设计当中，而在这种公众参与缺失和监督失效的情形下，更容易诱发算

〔12〕 参见张恭善：《立法学原理》，上海社会科学院出版社 1991 年版，第 62 页。

〔13〕 张文显：《法理学》，法律出版社 2009 年版，第 143 页。

〔14〕 参见黄信瑜、石东坡：《立法博弈的规制及其程序表现》，载《法学杂志》2017 年第 2 期。

〔15〕 参见杨炼：《论现代立法中的利益结构》，载《理论月刊》2011 年第 11 期。

〔16〕 参见陈鹏：《智能治理时代的政府：风险防范和能力提升》，载《宁夏社会科学》2019 年第 1 期。

〔17〕 参见张欣：《连接与失控：面对算法社会的来临，如何构建算法信任?》，载《法治周末》2019 年 5 月 30 日，第 12 版。

〔18〕 胡小明：《政府大数据应用效益反省》，载 https://www.chinathinktanks.org.cn/content/detail?id=hapu4w96，最后访问时间：2021 年 9 月 20 日。

法寻租和算法滥用问题。

二、立法性算法对立法程序的规避

（一）立法程序之于立法性算法的重要性

作为一种社会规范形式，法律的本质是对各种利益进行调节和分配，其终极目标是保障全民利益的相对均衡，而立法则是为实现利益均衡进行的制度设计和选择，立法过程也就被视为一个多重相互冲突的利益之间进行博弈和选择的过程。〔19〕在这个过程中，面对不同群体的利益诉求和相互冲突，立法部门不仅要对利益做出合理选择和价值取舍，还需要通过完善的制度安排使不同利益群体得以和谐相处。但是，现代社会是一个利益格局多元化的社会，由立法者代表立法已经越来越难以充分反映和实现不同民众之间的利益需求。一方面，由于立法是一项专门性活动，立法权只掌握在少部分人手中，但是，权力始终会存在被滥用的可能，而现代法治的基本要求是对各种权力，尤其是作为公共权力的立法权予以合法性和正当性的制约，从而防止权力不当使用。因此，寻求对立法权进行有效控制是现代法治要求的应有之义。另一方面，代议制民主不仅仅意味着“大多数人的统治”和“少数服从多数”，它还必须实现对弱势群体的保护以及对少数人的尊重。这就需要在一定程度上实现立法权的回归，以公众参与弥补立法代表在反映民意方面之不足。〔20〕对权力机关而言，保证公众亲历立法过程，可以在更加全面、客观和公正的把握民意的基础之上，最大限度地减少立法失误，实现立法的科学性和民主性要求。对民众而言，通过直接亲历立法过程，能够更加直观地表达自己的利益诉求，从而保障自己的监督权，这些在我国《立法法》的相关规定中都有充分的证明。

根据我国《立法法》第 4、5 条之规定，立法应当依照法定程序，体现人民意志，坚持立法公开以及保障人民通过多种途径参与立法。此项规定不仅具有传达并听取公众意见的形式意义，更重要的是它对保障公众参与和监督立法过程所切实发挥的作用具有实质性的意义。在美国，公众参与立法不仅比较普遍，而且所涉及范围也较广，基本包括宪法修改、国家基本法律的制定，甚至地方政策的出台都有公民参与其中。美国公众参与立法的合法性权利最早来源于《联邦宪法第一修正案》的相关规定，〔21〕此外，美国联邦程序法、〔22〕信息自由法以及联邦咨询委员会立法等法律规范文件也都对公民参与立法的合法性权利作出了明确而又细致的规定，并逐渐形成了集立法听证制度、公众评议反馈制度和立法信息公开制度“三位一体”的法律程序保护模式。尽

〔19〕 参见前引〔14〕，黄信瑜、石东坡文。

〔20〕 参见易有禄：《立法程序的功能分析》，载《江西社会科学》2010 年第 5 期。

〔21〕《美国联邦宪法第一修正案》规定：“国会不应当就设立宗教及其事务制定法律，也不应当通过制定法律限制公民的言论自由、新闻自由、和平集会的权利，以及向政府申请获得救济的权利。”它可以解释为赋予国会一项积极的责任，即为公民提供一种充分的机会，能够就公共事务进行有意义的讨论和辩论。而任何对公民为维护公共利益而实施的各种合法行为进行的限制或阻止均不受宪法保护，并且公民可以就此申请救济。

〔22〕《美国联邦程序法》第 552 条规定公众参与机制的规则制定情形，而第 553 条列举了不适用公众参与机制的规则制定情形。

管美国的现实国情和立法模式与我国有很大的不同，但法律的制定、修改以及实施等过程所追求的目标具有重叠性，即通过公众参与来保障立法过程的公开和透明。要言之，民主进程的推进需公众的普遍参与，他们须相互接触和了解，并通过公开讨论来参与公共生活，从而确定相互之间的共同利益并达成共识。〔23〕与此同时，公众的有效参与和监督还能以规范化的内部操作节省法律的外部执行成本，从而避免立法实践中的种种弊端。对阿伦特而言，公共政治生活需要人与人之间的相互辩论和理解，他们通过讨论和辩论确定共同的利益和价值目标，并努力实现这些目标，这种公开讨论能够使人们搁置争议、凝聚共识。〔24〕因此，强调公众对立法性算法程序的有效参与和监督具有实践必要性。

（二）立法性算法规避立法程序的危害性

算法通常被描述为通过“黑箱”将输入转换为输出，一般公众无法通过“黑箱”去理解这种转变如何发生，也不能用传统统计的直观和因果语言来描述这种关系。如果算法在公共决策领域的使用遭遇广泛质疑，也主要是因为算法与传统人类决策存有本质不同。首先，算法决策不能用人类所能理解的术语来进行解释，它不可避免地会不透明。其次，这些决策是基于大量数据识别的相关关系，而不是经证实的因果关系，在某种意义上还带有明显的随机性，因而不可避免地会出现错误。最后，算法决策不可避免地会反映特定群体的价值判断和选择，因而会带有较强的主观性。〔25〕这些特点以看不见的方式成为威胁现代民主法治框架的关键性要素。进一步而言，算法技术的专业特性还会对公众有效参与立法性算法程序设计造成阻碍。因为算法决策的形成通常包含对历史数据的收集与分析、为实现某个目标而构建模型和编码、为算法提供输入以及对输入数据的应用规定进行算法操作等流程。〔26〕这意味着那些无法产生数字数据的人可能会因此丧失参与公共事务讨论的重要机会。即使有，公众参与决策的过程也具有被动性或间接性，他们无法充分表达自己的利益需求和价值偏好，也缺乏必要的途径将其转化为立法选择。即使公众与立法机关之间存在直接沟通的数字交流平台，但“算法是一个随机的过程，不同变量之间往往会存在复杂的、不可预测的交互作用效应”〔27〕。换言之，算法“黑箱”的性质会对结果差异造成影响，这种可能性已被大多数学者和政策制定者所认识。更为重要的是，算法决策结果不能直观地被解释，也不能支持传统上立法机关对立法行为的背后因果关系进行辩护和说明。〔28〕这些都构成立法程序无法限制和约束立法性算法的重要理由。

然而，在算法治理过程中，“当国家获得数据产权和算法制定主导权，垄断了作为未来主要

〔23〕 See Czapanskiy K. Syma, Manjoo R, The Right of Public Participation in the Law-making Process and the Role of Legislature in the Promotion of This Right, 19 *Duke Journal of Comparative & International Law*, 1, 15 (2008).

〔24〕 See Saliternik Michal, Big Data and the Right to Political Participation, 21 *University of Pennsylvania Journal of Constitutional Law*, 713, 727 (2019).

〔25〕 See Berman Emily, A Government of Laws and Not of Machines, 98 *Boston University Law Review*, 1277, 1283 (2018).

〔26〕 See Brauneis Robert, Ellen P. Goodman, Algorithmic Transparency for the Smart City, 20 *Yale Journal of Law and Technology*, 103, 113－114 (2018).

〔27〕 Coglianese Cary, Lehr David, Regulating by Robot: Administrative Decision Making in the Machine Learning Era, 105 *Georgetown Law Journal*, 1147, 1172, 1199 (2017).

〔28〕 参见前引〔27〕，Coglianese Cary、Lehr David 文，第 1167 页。

公共产品的人工智能技术，并通过这种技术无限地干预社会，国家与社会的关系很大程度上将依赖于政府在推广和应用该项技术时是否遵循民主原则，并与社会进行广泛深入的协商”〔29〕。由于立法性算法并非立法者根据法定程序与公众平等对话沟通缔造之物，而是一种复杂的算法程序，并且立法文本也不是传统意义上的自然语言文本，而是非专业人士难以理解的人工语言文本，立法性算法程序的设计可能会面临公众参与的缺失和监督的失效，而在这种公众可参与性和可监督性降低的情况下，其不利影响可能更为明显。美国学者科恩曾将民主比喻为一种社会管理体制，在该体制中，社会成员大体上能直接或间接地参与公共决策。〔30〕就立法程序而言，公众参与是以公开的立法活动来保障那些可能受立法结果影响的普通民众，能够拥有平等的机会来参与立法的全过程，并对立法结果产生实质性的影响。这不仅关乎权力之间的分工和配合，也是公民权利对立法权力制约和限制的体现。

三、立法性算法何以规避立法程序

程序对法律制度的挑战由来已久，心理学家一直致力于运用程序正义原则来研究法律制度的公平感。顾名思义，程序正义只关注纠纷解决的程序性事项，而不涉及实质性结果，因而它与“实质”的公平无关，而与人们对公平的认识有关，是对人们所认为的公平程序的研究。程序正义的社会心理学研究揭示，“当法律权威无法让人们得到一个他们所期望的结果时，通过一个公平的程序来做出决定，更有可能获得人们的认可和接受”〔31〕。程序公开一直以来被视为是实现程序正义的基本标准和内在要求。就立法程序而言，程序公开要求立法过程和结果都要向社会公开，使公众能够亲历立法全过程，并为监督立法提供一种可能。作为程序民主的重要运行机制，公众参与的核心正是以一种较为完善的程序正义来确保实质正义，用公平正当的立法程序来保障立法结果的实质公正。程序正义在算法决策领域的研究发现，决定一个人是否相信某一特定算法程序的公平性有以下四个重要因素：（1）决策者是否以平等的态度对待他人与自己的互动；（2）决策者是否被认为是中立的；（3）决策者是否被认为是可信的；以及（4）个人是否有平等的机会参与决策过程。〔32〕如果运用这些因素来评估立法性算法，在算法未向公众充分披露、公众难以有效参与立法性算法程序设计过程之时，公众的程序正义感要大大降低。

（一）算法语言具有复杂性

算法是为实现特定行为而设计，必须按照给定的流程和轨道运行，其中包括构成算法的技术、

〔29〕 张春满、王震宇：《未来已来？人工智能的兴起与我国国家治理现代化》，载《社会主义研究》2019 年第 4 期，第 99 页。

〔30〕 参见〔美〕科恩：《论民主》，聂崇信等译，商务印书馆 1988 年版，第 10 页。

〔31〕 李昌盛、王彪：《“程序公正感受”研究及其启示》，载《河北法学》2012 年第 3 期，第 63 页。

〔32〕 See Ric Simmons, Big Data and Procedural Justice: Legitimizing Algorithms in the Criminal Justice System, 15 *Ohio State Journal of Criminal Law*, 573, 575－576 (2018).

工具和方法，它们有自己特殊的词汇、语法，以及编译单词、句子和文本的规则。〔33〕而语言正是由复杂的语义和句法结构的网、链和矩阵构成，它由基本符号、语形规则、语义规则三个部分组成。语言根据形成方式的不同可以分为自然语言和人工语言，前者可称之为日常语言，是人们在日常生活中在特定的语言范围内所反复使用的某种民族语。后者则是人类根据特殊需求而创造的符号或符号体系，其根本属性是人造语言。〔34〕算法正是借助于一套人工语言符号系统运用演绎体系以使其严格化的一套程序或方法，因此，算法语言属于人工语言的一种。但是，算法语言又与人工语言有很大不同，因为算法语言不是机器的符号表征系统，而是人类语言的符号表征系统。〔35〕在其符号表征系统的最基本层次上，计算机只能有两种状态，即存在或不存在某种电磁现象。它可以处理任何信息，无论是文字、图形或声音，这些都可以用二进制数字符号在计算机程序中得以表示。〔36〕数字是计算机领域运用的一种基本语言，它们与技术有着千丝万缕的联系。布尔逻辑与二元数字的融合形成了计算机设计的基本结构，它蕴含了三个基本运算 and、or 和 not，主要处理两种实体，比如 true 或 false，yes 或 no，open 或 closed，on 或 off，0 或 1。当程序按照布尔原理予以排列时，其能创建一种既可以执行数学运算又可以执行逻辑运算的电路。算法主体能够通过借助计算机程序来完成复杂的社会治理目标，这些目标由机器翻译成一个庞大的目录，其中包含所有可能场景的简单命令。在算法世界里，这些指令被认为是算法主体依据治理目标以及个体行为来进行校准的。〔37〕例如算法主体可能越来越依赖由大数据支持的方法来定制微观指令，或通过数据化分析对社会主体进行自动化监管，而不是依据法律或一般规则。

语言是一种信息交换的符号系统。哈贝马斯将交往活动视为以符号为媒介的相互作用和理解，而“相互作用是按照必须遵守的规范进行，它规定着相互行为的期待，并且必须得到至少两个行动主体（人）的理解和承认”〔38〕。虽然“语言是人们按照一定的规则表达和交流自己思想意志的工具，而立法语言作为表达法律规范内容的唯一工具，只能以特定的语言形式而存在”〔39〕。但构成立法性算法的人工语言对普通公众而言难以理解。因为信息在人和机器之间至少需通过三个层次的传递，每个层次都有其独特的语言，第一层次是机器可读的二进制语言，第三个层次是只有人类才能理解的自然语言，连接这两个层次的是一组人和机器都能理解的编程语言。〔40〕而公众参与立法中的“公众”应该是一个能够自主表达和接受意见，并能够自觉、自主地参与讨论

〔33〕 See Alexey V. Lisachenko, Law as a Programming Language, 37 *Review of Central and East European Law*, 115, 118 (2012).

〔34〕 参见胡泽洪：《现代逻辑视野中的语言与思维》，载《哲学研究》1997 年第 6 期。

〔35〕 关于符号表征系统，皮亚杰认为符号表征是认知发展的核心，是指个体用来代表其他事物的东西，符号表征能力是人类所独有的一种能力。

〔36〕 See J C. Smith, Machine Intelligence and Legal Reasoning, 73 *Chicago-Kent Law Review*, 277, 279 - 280 (1998).

〔37〕 See Casey A. Niblett A, The Death of Rules and Standards, 92 *Indiana Law Journal*, 1401, 1405, 1418 (2017).

〔38〕〔德〕尤尔根·哈贝马斯：《作为“意识形态”的技术与科学》，李黎等译，学林出版社 1999 年版，第 49 页。

〔39〕 前引〔12〕，张恭善书，第 254 页。

〔40〕 See Anne von der lieth Gardner, An Artifificial Intelligence Approach to Legal Reasoning, MIT Press Cambridge, 1987, pp. 24 - 26.

并影响立法决定的普通群体。〔41〕这就需要以同等的语言作为沟通媒介。法律虽是以特定话语进行程式化的表达，构成立法性算法程序的人工语言和自然语言之间存在的差别，在某种意义上可以视为专家话语和公众话语在立法互动过程中的差别。然而，作为一种利益协调和分配机制，法律还必须与社会其他制度相互联结。特别是，在自然语言交流中它还必须寻求与任何可能存在的人际交往建立确定的联系。〔42〕就立法性算法而言，如果过度关注人工语言的一般性，而忽视自然语言的内在特性，以及它在促进人际交往和实现制度安排方面的价值和意义，往往容易导致公众在算法程序设计过程中的缺失。而一旦大数据与人工智能成为立法权力机关的主要信息来源，作为民主性补充渠道的公民立法参与机制将较难发挥作用，这是因为公民由于不具备与此相关的专业知识，而无法表达其利益或反驳相应的科学依据，即使表达出与之相反的意见也可能被斥以误解科学技术的立法依据〔43〕。因此，在算法治理之下，协商式民主的真正难题可能并非在于保证不同利益群体达成共识，而在于如何跨越自然语言和人工语言之间的鸿沟，为公众参与立法提供一个能够平等对话和沟通的桥梁。

（二）算法决策具有非中立性

在算法决策中，表面上中立的算法可能会产生社会实质性的偏见结果。因为，“技术本身是一种带有明显偏向性的思维和结构（structure），它影响和塑造了形形色色的‘行动者’（agent），而技术的后果往往也会超出人们的原初设定”〔44〕。尽管算法决策的产生可能遵循相同的程序规则，但它仍会强化系统中业已存在的偏见和误差。在特殊情况下，算法对输入数据做出的假设并不总是正确，也并非总是按照设计者的预期进行运作。无论这些因素是故意还是偶然所致，算法总会或多或少地受到个人或集体偏见的影响。例如，在算法程序的价值渗入上主要存在两种路径，“一是程序开发人员在设计算法时，参数设定会受到主观价值偏好的影响；二是用户在使用智能设备之时，可以根据自己的需要设置相应的算法应用参数”〔45〕。而在一个复杂算法程序中，算法的实际偏差很可能是由不同程序员指定的规则组合而成的，单个程序员的偏见通过汇集可能会产生更大的累积效应，由此作出的决策虽然能够有效代替传统人脑的决策形式，但也可能会使其遭受质疑。此外，数据挖掘对算法偏差也特别敏感，为确保数据挖掘揭示的模式比分析中的特定样本更适用，样本必须按比例代表整个人群。〔46〕一旦某个样本中包含特定类别不成比例的代表，那么该样本的分析结果可能偏向于支持或反对代表过多或不足的类别。因此，将算法视为客观中立的想法实质上会掩盖算法内部运行的复杂情况，会忽视算法内部逻辑的系统性和结构性不公平因素，同时也会对算法的非中立性技术

〔41〕 参见王怡：《认真对待公众舆论——从公众参与走向立法商谈》，载《政法论坛》2019 年第 6 期。

〔42〕 See Waldron Jeremy, Law and Disagreement, Oxford University Press, 1999, p. 105.

〔43〕 参见钱大军：《立法权回收中人工智能的应用及其悖反》，载《上海师范大学学报（哲学社会科学版）》2019 年第 6 期。

〔44〕 袁光锋：《政治算法、“幻影公众”与大数据的政治逻辑》，载《学海》2015 年第 4 期，第 51 页。

〔45〕〔美〕温德尔·瓦拉赫、科林·艾伦：《道德机器：如何让机器人明辨是非》，王小红等译，北京大学出版社 2017 年版，第 1 页。

〔46〕 See Solon Barocas, Andrew D. Selbst, Big Data's Disparate Impact, 104 *California Law Review*, 671, 686 (2016).

特性缺乏清醒的认识。

事实上，立法性算法同样并非具有中立性，一旦算法程序只是由特定主体控制产生，那么据此作出的决策，其公平性和合法性就将大大降低。因为公共决策的产生不能仅仅代表某一群体价值偏好或利益取向的简单集合，它须是受影响者之间真正协商的结果，其中包括交流合理的观点和建议以及共同寻求解决问题的办法，这种协商模式能够强化参与者的能动性和自我实现，同时也能保证决策的科学性和民主性。在桑斯坦看来，协商可以聚合信息和观念，使群体作为一个整体比其最好的成员知晓更多，做得更好，而协商的一个关键目标就是确保能够获得广泛分散的信息，并将其纳入公共决策系统之中。〔47〕虽然算法技术的诞生是为了将无限包围在有限之中，但算法“黑箱”的出现却加深了人类对算法运行过程中数据输入或输出的认知盲点，从而打开了通向无限的大门。〔48〕在立法领域，传统立法权能够受到宪法、法律或社会公众等诸多力量的有效监督和制约，而立法性算法的生成过程则对这些限制性力量构成了突破，并有可能规避来自后者的制约和限制，这是人类可能面临的新难题。

四、立法性算法的程序再规范

在当下，有权机关利用算法可以较为快速、准确地掌握社会公众关注的焦点问题，并能真正了解社会公众的真实需求，从而提高社会治理效率并推动国家治理绩效的改进，以及改变部分领域的治理格局。〔49〕但是，数据输入和输出、程序的设计也有可能会受到特定主体的影响和控制，使得受算法影响的主体被排除在参与和监督的程序之外。为避免由此可能产生的不利后果，立法性算法的产生必须在遵循法定的程序要求下进行。与传统立法中的立法公开、公众参与、社会听证等制度所能带来的效果类似，公开透明及其问责两个维度的算法治理目标同样可以在保障公众参与和监督算法程序设计上发挥重要作用。

（一）通过算法公开保障公众对立法性算法的参与

立法程序对立法性算法的再规范应当要求算法公开透明，这成为立法性算法规制领域的一个原则性建议。算法治理目标的实现最终能否获得理想效果，取决于公众是否能够准确、及时地获取有效的算法设计信息，并能对其决策内容展开自由和公开的辩论。因此，权力机关在使用算法之前，应当严格遵照《立法法》第5条关于立法公开、公众参与相关规定之要求。一方面，根据立法公开的基本原则，算法程序需要披露相关算法规则，其中包括正在优化的目标函数、用于优化的方法以及算法的输入变量和源代码，如此方能保证公众对算法程序设计的知情权，从而有利于社会公众（尤其是专业人士）针对立法性算法实施监督，以及对算法决策提出公平性和合理性质疑。另一方面，算法程序的设计既要注重公众的形式参与，同时也要注重公众的实质参与，公众意见在立法性算法程序中得以反映则是公众参与的实质性表现。国外学者

〔47〕 参见〔美〕桑斯坦：《信息乌托邦》，毕竟悦译，法律出版社2008年版，第52－56页。

〔48〕 See Erika Giorgini, Algorithms and Law, 5 *Italian Law Journal*, 131, 148, 149 (2019).

〔49〕 参见陈鹏：《算法时代的国家治理：在算法与法律之间》，载《法治社会》2019年第6期。

认为通过引入“法律设计”〔50〕思维的概念，将用户的意见集中于嵌入算法系统之中，以确保技术解决方案从一开始就设计为满足法律技术终端用户的需求，〔51〕以此提升公众对算法程序设计的参与感。作为一种评估和创建法律服务系统的新模式，它主要通过对算法的过程、思维方式和机制的控制来帮助人类构建和测试更好的法律行为模式，从而使非技术专业群体都能参与其中并获得授权。〔52〕

另外，随着公众需求的多样化、利益主体的多元化以及立法技术的复杂化，有效的公众参与既要重视个体化的单方参与，同时也要重视组织化的社会参与。前者能为个人发表意见提供平等对话沟通之平台，而后者能够弥补个体因知识欠缺、能力不足导致立法参与缺失之不足。一方面，鉴于算法决策有可能加剧新的社会分层和拉大不同社会群体的差距，其程序的设计至少必须为那些生活在数据流之外的边缘群体提供保障，保证那些数据足迹较小的群体在分配公共产品或服务之时有足够的发言权，以致不会受到算法的不平等对待。〔53〕与此同时，还应当保证算法决策须是根据同一套特定程序产生，并在每种情况下都平等一致地适用于任何人。因为对特定程序的遵守能够代替那些对公民权利义务产生实质性影响的算法决策产生的严格证明，并确保算法决策的产生是依赖于同样的一套技术标准。须注意的是，算法程序设计的公开虽然能够为公众参与大开方便之门，但并不意味着所有人都能够平等参与其中，即使可以，也会因流于形式而违背立法公开制度设计的初衷，而公众参与算法程序设计的实际效果也会大大降低。由于算法所包含的知识内容通常比较晦涩难懂，鉴于算法技术的专业性和算法语言的特殊性，在很多情况下，缺乏必要专业知识基础的普通公众很难参与到立法性算法程序设计当中。对此，可通过引入“交流型专家”〔54〕来协助技术内核部分，“在专家和公众之间实现知识传递和共识达成，并在决策过程中细化和具化公众参与的能力，从而保障公众的实质参与”〔55〕。作为连接公众和权力机关的中间桥梁，“交流型专家”的作用在于将一些难以理解的算法人工语言向普通公众进行传递，并对算法程序的设计提出专业性的意见和建议。〔56〕

在科学技术与民主关系的认知、判断与冲突之中，公众对立法性算法程序设计的有效参与，还须保证其拥有掌握或了解算法技术的基础知识与判断能力，从而为立法性算法的民主化和科学化发展提供必要的条件，这既是在人工智能时代保持公众独立思考和批判能力的基本要求，也是应对社会治理领域算法化方向转变的重要举措。因此，注重立法方法和

〔50〕 斯坦福大学法律设计实验室的玛格丽特·哈根是最早提出“法律设计”一词的人之一。哈根将其定义为一种以用户为中心的意识形态，被视为实现以人为中心的设计的过程、思维方式和机制集。

〔51〕 See Toohey Lisa、Moore Monique，Dart Katelane，Toohey Dan，Meeting the Access to Civil Justice Challenge：DigitalmInclusion，Algorithmic Justice，and Human-Centred Design，19 *Macquarie Law*，133，153（2019）.

〔52〕 参见前引〔51〕，Toohey Lisa、Moore Monique、Dart Katelane、Toohey Dan 文，第 153－154 页。

〔53〕 See Lerman Jonas，Big Data and Its Exclusions，66 *Stanford Law Review Online*，55，61（2013－2014）.

〔54〕 谭笑：《技术问题决策中的专家话语和公众话语——柯林斯（重思专能）的方案》，载《开放时代》2014 年第 6 期，第 220 页。

〔55〕 前引〔54〕谭笑文，第 220 页。

〔56〕 See Danielle K. Citron，Technological Due Process，85 *Washington University Law Review*，1249，1312（2007－2008）.

观念的时代转变，培育公众对立法性算法程序设计的参与技能，增强公众的民主参与意识也显得尤为重要。

（二）通过算法解释保障公众对立法性算法的监督

事实上，对于涉及一些随机因素的决策过程，即使是系统源代码、输入、操作环境和结果的完全透明，也不能排除结果可能以不可检测的方式被错误地固定的可能性。〔57〕算法的语言和操作系统对于普通民众来说非常难以理解，即使专家也常常难以理解算法程序的全部运行过程。因此，算法公开对于保障公众有效的参与和监督而言，其作用范围十分有限。在此基础之上，学界普遍认为通过设计算法责任机制来促使利益相关者实现问责的目标，同样能达到监督和约束效果。算法问责体现为算法解释，它能让算法决策相对人有机会在充分知情的情形下主张自己的权利，并要求算法控制者以自然语言或可视化技术对算法逻辑尤其是输入数据与输出结果之间的相关性进行解释。〔58〕就立法性算法的解释而言，则表现为算法主体对算法决策产生逻辑的解释要清晰、合理和言之有据，不能违背宪法、法律相关规定的基本要求，并在算法解释程序上能够妥善处理公众可能提出的质疑。

传统上，立法解释的目的主要服务于法律实施，立法解释工作是通过阐明法律概念、填补法律漏洞以及探究立法原义等方式，来促使存在争议的法律规则能够得以有效实施。而对立法性算法进行解释的原理同样在于，通过赋予公众获得关于立法性算法解释的权利，以明确权力机关的解释义务和技术责任，提高算法的透明度和公众参与度，实现权力主体的可归责性和公众权利的可救济性，从而推动立法程序和立法性算法的深度融合，最终能够形成利益均衡、公平一致的算法决策。作为一种对算法决策产生过程公开原则之不足的补救办法，对立法性算法的解释既直观地表现为一种打开“黑箱”的手段，通过公众对算法程序的参与和监督允许公众对算法决策提出质疑和纠正，同时也为公众权利救济提供一种必要的途径。然而，作为一种事后的规制手段，对算法进行解释必须受到立法程序的严格限制。因为根据权力的性质和层级不同，其解释的主体和程序以及解释的效力也有所不同。因此，立法性算法解释的相关程序设置理应在立法解释的框架范围内进行。

五、结　语

在现代民主社会里，社会正义和制度正义的实现要求保障和促进不同利益群体以合法的形式进行立法需求的表达和主张。而立法程序的意义就在于限制和消除立法活动中的恣意因素，广泛听取和接纳不同群体的主张，以协调不同群体之间的利益冲突，进而制定出体现实质正义的法律。尽管当下人们还无法对算法程序的设计和应用进行有意义的控制，但立法性算法与一般算法不同，它的产生必须严格依照立法程序的相关规定进行，保证公众对立法性算法程序设计全过程

〔57〕 See Joshua A. Kroll, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson, Harlan Yu, Accountable Algorithms, 165 *University of Pennsylvania Law Review*, 633, 650 (2017).

〔58〕 参见解正山：《算法决策规制——以算法“解释权”为中心》，载《现代法学》2020 年第 1 期。

的知情、参与和监督。这既是保障公民权利的重要体现，也是实现算法决策民主化和科学化的关键环节。因此，要实现立法程序对立法性算法的再规范，就要求算法程序的设计必须以公开透明和问责制为主要原则，以确保公众对立法性算法的充分参与和必要的权利救济。

Abstract: Legislative algorithm means public decision algorithm formulated by authorities in accordance with certain procedures, which even have a substantial impact on citizens' rights and obligations. Just like traditional legislation, legislative algorithm will change the distribution patten of social resources and people's space, also, legislative algorithm have a substantial impact on the citizens' rights and obligations. However, legislative algorithm may base on the inherent technical characteristics to avoid the public participation and supervision of legislative algorithm programming. On the one hand, there is a big difference between the artificial language that constitutes legislative algorithm with the natural language, which familiar to the general. Because the general public doesn't have the knowledge of artificial language, it's difficult for them to get an equal dialogue and effective communication in the algorithmic programming, which may cause the problem of power-responsibility imbalance and supervision failure. On the other hand, the legislative algorithm embed the designer's preferences and value judgments unconsciously, and it can't fully demonstrate the objectivity and truth under the ideal of "technology neutrality", and even may produce deviations, which may lead to the problem of algorithm abusing and algorithmic bias. In order to overcome these shortcomings, it's required that the design of algorithm programs must take transparency and accountability as the main principles to ensure the full participation of the public in legislative algorithm and provide necessary rights remedy.

Key Words: legislation, algorithm, legislative procedure, legislative algorithm, public decision algorithm

（责任编辑：于文豪　赵建蕊）

财经法学 No. 3，2022
pp. 29 - 42

论数字时代的美术作品原件
——基于展览权的视角

李　强*

内容提要：美术作品原件是我国著作权法上展览权的核心概念，然而却未得到应有的关注。面对新技术、新业态提出的新挑战，无论是传统美术作品还是数字化美术作品，都存在着如何理解和认定美术作品原件的困惑。对此，有必要突破著作权法上关于美术作品必有原件、美术作品原件唯一和美术作品原件必为实体等传统认识，顺应技术发展的要求，紧紧抓住可展览性和不可替代性两个关键特征来构建美术作品原件的概念，并创建认定美术作品原件的一般规则。对于数字化美术作品，在满足“间接”可展览性的前提下，可以借助 NFT 技术将数字化美术作品完成时所形成的电子文档认定为作品原件。

关键词：美术作品　作品原件　展览权　NFT

一、问题的提出

在众多著作财产权当中，展览权只是一个不起眼的小权利，但在现实生活中却有着大应用。近几年来，我国文博事业取得了大发展、大繁荣，从法律的角度而言，其兴旺发达最重要的权利基础就是展览权。我国著作权法上的展览权正是基于美术、摄影作品的原件或复制件（以下或简称为“作品原件或复制件”）而定义的，即“公开陈列美术作品、摄影作品的原件或者复制件的权利”（《著作权法》第 10 条第 1 款第 8 项）；与展览权相关的第 20 条则几乎是作品原件的定制条款，[1] 可见作品原件在展览权中的重要性。

* 李强，武汉大学图书馆/万林艺术博物馆馆员。

本文为国家社科基金项目“当前国际版权制度发展趋势与我国路径选择研究”（17BFX117）、国家市场监督管理总局发展研究中心项目“数字经济时代知识产权保护与反垄断规制创新研究”的阶段性成果。

〔1〕《著作权法》第 20 条第 1 款规定作品原件所有权转移后原件展览权的归属，第 2 款解决原件受让人展览未发表的作品原件与作者发表权之间的冲突。

文化生活中，展示原件是举办文博类展览的基本要求和行业惯例，特别对美术作品而言更是艺术家展现创作才能、提高艺术声誉的主要途径，亦是美术作品实现艺术价值的主要方式。司法实践中，早年的“蔡迪安等与湖北晴川饭店有限公司等著作权侵权纠纷上诉案”（即《赤壁之战》壁画案）〔2〕曾引发大量的学术讨论，案件起因即为绘制于饭店墙壁上的唯一壁画原件遭到毁损灭失。近年来，再次引发诸多学术兴趣的“钱钟书书信拍卖案”〔3〕和“茅盾手稿拍卖案”〔4〕也聚焦于两位先生的手稿原件及其展览权，引来法院判决和学者观点的分歧甚至对立。〔5〕还有判例将“音乐喷泉喷射效果的呈现”认定为美术作品，〔6〕那么音乐喷泉的喷射就是在公开展示美术作品，学者对此也表示了明确的反对意见。〔7〕作为展览权的主要客体，如果充分认识到美术作品原件的展示并不限于美术馆、博物馆、会展中心等专门场馆，还包括商场（含任何借助展示美术作品而进行营销的现场）、酒店、宾馆甚至街道等数量庞大的公众场所，〔8〕那么，讨论美术作品原件既有重要理论价值又有重大实践意义，也充分展现了本文研究的问题导向。

然而，从法学角度对美术、摄影作品原件展开的研究非常少见。目前有限的国内研究主要集中在对现行《著作权法》第 10 条第 1 款第 8 项（展览权的定义）和第 20 条第 1 款〔9〕的理解与适用上。比如，作品原件转移后原件展览权的归属，〔10〕作品原件转移后由原件所有人享有原件展览权则引出了作品原件所有权和作品著作权之间的冲突与协调〔11〕。英文领域的研究则主要关注在公共场所展示宗教物品的政教分离条款（the establishment clause）或展示艺术品的言论自由等美国宪法第一修正案，〔12〕以及数字图书馆、Twitter 等社交平台的网上展示，〔13〕极少提及作品原件或复制件。

〔2〕 参见湖北省高级人民法院（2003）鄂民三终字第 18 号民事判决书。

〔3〕 参见北京市第二中级人民法院（2013）二中保字第 9727 号民事裁定书。

〔4〕 参见江苏省南京市中级人民法院（2017）苏 01 民终 8048 号民事判决书。

〔5〕 参见金海军：《论书信上的物权、著作权与隐私权及其相互关系——从“钱钟书书信拍卖案”谈起》，载《法学》2013 年第 10 期；李翔、曹雅晶：《失落的展览权——从“钱钟书书信拍卖案”谈起，兼论〈著作权法〉第十八条之理解》，载《中国版权》2014 年第 4 期；石超：《手稿著作权客体类型探究——基于“茅盾手稿案”的分析与思考》，载《中国出版》2019 年第 1 期；陈瑞雪：《论文字作品的亲笔手稿著作权保护问题——以茅盾先生手稿著作权纠纷案为例》，载《福建法学》2019 年第 1 期。

〔6〕 参见北京知识产权法院（2017）京 73 民终 1404 号民事判决书。

〔7〕 参见王迁：《论作品类型法定——兼评“音乐喷泉案”》，载《法学评论》2019 年第 3 期；李扬：《著作权法基本原理》，知识产权出版社 2019 年版，第 72 页。

〔8〕 相关案例可参见北京市第二中级人民法院（2003）二中民终字第 5951 号民事判决书；北京市东城区人民法院（2007）东民初字第 03991 号民事判决书；湖北省武汉市中级人民法院（2010）武知初字第 66 号民事判决书；天津市第一中级人民法院（2016）津 01 民终 6756 号民事判决书。

〔9〕 该款规定：“作品原件所有权的转移，不改变作品著作权的归属，但美术、摄影作品原件的展览权由原件所有人享有。”

〔10〕 参见李明德、管育鹰、唐广良：《〈著作权法〉专家建议稿说明》，法律出版社 2012 年版，第 97－98 页；郑成思：《版权法》（上），社会科学文献出版社 2016 年版，第 321 页。

〔11〕 参见王福珍：《作品原件所有权与作品著作权的冲突及解决方案》，载《法学》1993 年第 9 期；郭玉军、向在胜：《论美术作品著作权与原件所有权》，载《湖北美术学院学报》2001 年第 3 期；唐昭红：《论美术作品著作权对美术作品原件所有权的限制》，载《法商研究》2003 年第 4 期。

〔12〕 See Christina A. Mathes, Bery v. New York: Do Artists Havea First Amendment Right to Sell and Display Art in Public Place? 5 *Villanova Sports & Ent. Law Journal*, 103 (1998); Susan L. Trevarthen, Johanna Lundgren, Merry Litigation and Happy Attorney's Fees: Holiday Display on Downtown Public Property, 85 *Florida Bar Journal*, 19 (2011).

〔13〕 See David R. Hansen, The Public Display of Digital Library Collections, 14 *N. C. Journal of Law & Technology*, 145 (2012); Jie Lian, Twitters Beware: The Display and Performance Rights, 21 *Yale Journal of Law & Technology*, 227 (2019).

笔者在梳理这些研究时发现一个令人困惑的现象，即围绕展览权或美术作品原件展开的探讨似乎将美术作品原件本身当成一个不用言说、不言而喻的概念。但是，越来越多的艺术创新对这种“想当然”提出了有力的挑战。比如，用无人机编队或烟花燃放形成的艺术造型，用蘸水的笔在地面上写出的书法，还有将发型认定为立体美术作品的判例。〔14〕在这些美术创作中，什么是美术作品的原件，美术作品是不是必有原件？人类已经进入数字社会，元宇宙也开始占据大众的视野，数字财产的价值和重要性渐次攀升。传统时代，美术作品的原件是有体物；数字时代，作为一种数字财产形式，数字美术作品的原件又是什么？近两三年来，越炒越热的 NFT（non-fungible token，不可互替通证或非同质化代币）艺术作品逐渐成为数字时代收藏界的新宠和吸引流量的焦点，时不时报道出来的巨额拍卖令人咋舌。NFT 艺术作品即为经由 NFT 技术加持的数字美术作品，那么，使用画图软件在电子屏幕上绘制一幅美术作品，呈现在屏幕上的画面，由该作品形成的电子文档，存储电子文档的内存模块或硬盘、光盘，还有制作出来的第一份纸版作品，哪一个是原件？

为此，本文在辨析作品原件和作品载体之间关系的基础上，从实践出发，基于展览权的角度纳入适当的考量因素，构建了可以兼顾传统美术作品和数字美术作品的美术作品原件概念，并创建了认定美术作品原件特别是数字美术作品原件的若干规则。

二、作品原件和作品载体的关系辨析

根据我国著作权法，展览权的客体是美术作品和摄影作品，客体的载体是作品原件或复制件（以下或简称为“作品制件”），其本身也是物权的客体。

（一）作品载体学理分类的局限性

通说认为，作品必须通过一定的形式表达，才能被他人感知；采取一定的形式固定，才能得到法律的保护。这不仅是作品创作的本质属性和实际需要，也是国际条约（《伯尔尼公约》第 2 条第 2 款）和相关立法例为作品提供法律保护的基本要求。这种固定的形式就是作品载体。

根据物理特性不同作品载体可以分为固定载体和瞬间载体，前者指有形的物质实体，后者指无形的物质，如口头作品之声波、表演作品之动作，数字作品的无形载体是电子脉冲。根据是否为首次依附分为原始载体和复制载体，前者又称原件，“是作品最初所附的载体”，后者又称复制件，“是承载原始载体上之作品的载体”〔15〕。

然而，与实践对比不难发现，除了通过最传统的纸笔或刻刀等方法创作的如著作手写稿、绘画、雕塑等作品外，上述原始载体和复制载体的分类不能直接用于确认作品的原件或复制件。比如，用计算机撰写的著作，其原始载体是电子脉冲，复制载体是硬盘、优盘等存储器，但什么是该作品的原件却颇费思量。再如，口述作品的原始载体是无形的声波，复制载体是固定声波的磁带；而在大众认知中，录音棚或现场录制的母带是原件，从母带翻录的都是复制件。

〔14〕 参见“何吉与杭州天蚕文化传播有限公司著作权纠纷上诉案”，浙江省杭州市中级人民法院（2011）浙杭知终字第 54 号民事判决书。

〔15〕 杨述兴：《论作品与载体的关系》，载《知识产权》2012 年第 6 期，第 42 页。

所以，作品载体的上述分类主要是一种学理认识，不能满足实践的需要。真正具有法律意义的作品载体是固定载体或称为实体载体，如《著作权法》及实施条例多次提到的作品原件或复制件。具体到美术作品原件亦是如此，比如，“美术作品的‘原件’，也就是通常所说的‘原稿’，或者是‘原本’、‘底本’”〔16〕；“美术作品必须被固定在物质载体上，不能像口述作品那样脱离物质载体而存在，否则也不可能有‘原件’和‘复制件’的区分了”〔17〕。

（二）其他作品原件和美术作品原件在司法实践中存在重要差异

从司法实践来看，对于美术、摄影作品以外的其他作品，作品原件的法律意义主要体现在由于没有备份而毁损丢失时会导致整个作品的灭失。比如，在被称为国内首例教案纠纷的“高丽娅诉重庆市南岸区四公里小学著作权纠纷案”中，〔18〕被告弄丢了原告 12 年间历次上交的大部分教案本（无备份）。其实，即便原告诉称被告遗失其作品原件系侵犯了其著作权，法院仍倾向于将之认定为侵犯了原告对作品原件的所有权，如“沈金钊诉上海远东出版社图书出版合同案”〔19〕和“邱传海与湖北电视剧制作中心等返还作品赔偿纠纷案”〔20〕（以下简称“邱传海案”）。在这两个案例中，原告的诉求都包括追究被告遗失其作品原件的著作权侵权责任，但是终审法院都没有支持原告的诉求，而是认定为涉及作品原件的财产权纠纷进行判决。

就美术、摄影作品以外的其他作品原件而言，从上述及类似案例可以得出三个重要推论。一是如果存有复制件，作品原件是否丢失无关紧要。二是如果缺乏复制件，作品原件的作用主要体现为是作品的唯一载体，一旦灭失即意味着整件作品的灭失，至于是什么形式的载体并不重要。三是作品原件彰显的主要是使用作品的财产价值，而不是其本身的价值。比如，在邱传海案中，原告就诉称由于被告遗失其唯一的相关手稿原件，导致有关合作方取消了原告书籍的出版和电视剧的拍摄，造成了财产损失。

但是，如果涉案作品原件有可能构成美术作品原件，则不仅会关联展览权，而且侵权认定的性质也完全不同。比如，在“钱钟书书信手稿拍卖案”和“茅盾手稿拍卖案”中，法院判决和学理研究均认为，在著作权法上，钱钟书先生和茅盾先生的手稿既是文字作品又是书法类美术作

〔16〕 李建国主编：《〈中华人民共和国著作权法〉条文释义》，人民法院出版社 2001 年版，第 136 页。

〔17〕 前引〔7〕，王迁文，第 24 页。

〔18〕 原告原为被告所属教师，每学期按照被告的安排编写和上交教案，自 1990 年至 2002 年先后交给被告教案本 48 册。在原告要求返还教案本后，被告只返还了 4 册，其余 44 册被被告以销毁或者变卖等方式处理，下落不明。原告起诉被告要求其返还教案本并赔偿经济损失。原告在以物权纠纷起诉、上诉和申诉均败诉后，转以著作权纠纷为由起诉，最终胜诉。参见重庆市第一中级人民法院（2005）渝一中民初字第 603 号民事判决书；重庆市第一中级人民法院（2005）渝一中民再终字第 357 号民事判决书。

〔19〕 原告按照出版合同约定将其唯一的手稿原件交由被告出版社出版，后被告将手稿的前两千页遗失。原告诉求之一即为被告侵犯了其对手稿原件的著作权。一审法院支持了原告请求，但二审法院认为被告侵犯了原告对书稿原件享有的所有权而非作品著作权。参见上海市第一中级人民法院（1997）沪一中民终（知）字第 1469 号民事判决书。

〔20〕 20 世纪 80 年代后期至 90 年代，原告在先后三次参加被告组织的职称评审过程中，提交了包括文学剧本、电视剧分镜头剧本和著作手稿在内的大量作品手稿，绝大多数没有备份。评审结束后，原告多次向被告索要手稿材料无果，遂诉至法院。虽然湖北省检察机关在办案过程中找到了部分手稿（约 150 万字）并发还作者，但仍有 70 余万字的手稿材料没有找回。该案历经区、市、省三级人民法院和最高人民法院多次审理，原告虽然胜诉，但是湖北省高级人民法院的再审判决没有认可原告提出的著作权侵权主张，最高人民法院的再审判决也没有认可最高人民检察院提出的著作权侵权的抗诉意见，而是认定该案为“主张返还作品手稿原物及赔偿损失的物权纠纷”，维持了湖北省高级人民法院的再审判决。参见湖北省高级人民法院（2009）鄂民监二字第 10 号民事判决书；最高人民法院（2012）民抗字第 50 号民事判决书。

品，后者即为展览权的客体。〔21〕在这一类案例中，被告的涉案行为在侵犯原告物权的同时也可能侵犯了著作权，法院还需要判定被告公开展示美术作品原件的行为是否侵犯了原告的展览权。换言之，在涉及美术作品原件的案例中，即使存有海量复制件，作品原件本体的毁损或丢失即属于重大损失；作品原件本体不存，与其不可分离的原件展览权也归于消灭。

所以，上述针对其他作品原件的三点重要推论不能类推适用于美术作品的原件。主要原因在于美术作品与美术作品原件不可分离，以及美术作品原件所具有的可展览性。应该说，这两点都是美术作品原件的本质属性，且可展览性既是现行立法赋予美术作品原件的法律属性，又是其区别于其他作品原件的关键特征。《美国版权法》第 101 条定义的“公开展示权”不仅包括直接展示，还包括通过胶片、幻灯片、电视图像或任何其他设备或程序展示作品的载体；换言之，既包括直接展示和间接展示，也包括现场展示和网上展示。与之相比，一方面，我国的展览权定义没有使用诸如“借助其他任何设备或方法”的用语，应当是“直接展示”作品的载体即原件或复制件，不包括“间接展示”。另一方面，在我国著作权法的架构中，现场播放视频的展示行为适用放映权，现场网上展示作品适用信息网络传播权，只有现场直接展示作品原件或复制件本身才适用展览权。所以，在我国著作权法的语境下，美术作品原件的可展览性就是指不需要借助任何设备或方法在现场直接展示原件本身亦即作品载体。

对于传统美术作品如绘画、书法、雕塑等，不论原件还是复制件都具有可展览性，展示作品载体就是展示作品本身，作品原件就是作品的原始载体，复制件就是复制载体。对于数字化美术作品，展示储存作品电子文档的内存模块或硬盘、光盘等载体不能得到展示作品的效果，即这些载体不具有可展览性，不能认定为展览权意义上的原件或复制件，尽管可以作为作品的原始载体或复制载体。所以，有学者指出，“‘原件’这一概念仅于传统创作形式的美术作品之上才有意义，才能体现出原件与复制件之差异”〔22〕。摄影作品存在同样的问题，传统的胶卷可以作为原始载体，但不能作为原件；数码相机里的存储卡可以作为原始载体，也不能作为原件。正是因为数字化美术作品的原件和载体之间的关系迥异于传统美术作品，才导致不易判定数字化美术作品的原件，这也是技术的发展对著作权立法提出的具体挑战。所以，在构建美术作品原件的概念和创建美术作品原件的认定规则时，必须将数字化美术作品的特殊性纳入考量。

三、构建美术作品原件的概念

（一）两个重要区别

1. 美术作品原件与复制件的区别

无论对创作者、观赏者还是所有者而言，美术作品的原件和复制件在价值上相差悬殊，本身存在着质的不同。尤其是作品原件与作者之间存在着强烈的人身联系，在精神和经济上均具有特殊重要的价值，蕴藏着作者最原初的艺术才情、创作技巧和身心投入，不能为复制件或任何同主题的再

〔21〕 参见前引〔5〕，金海军文；前引〔5〕，陈瑞雪文。

〔22〕 杨明：《文字作品 v. 美术作品：对几个基本理论问题的反思》，载《中外法学》2009 年第 2 期，第 261 页。

创作所替代，与美术作品不可分离。在文博行业，不论是文物还是艺术品，以展览真品和原件为基本原则和最低要求，观众也以欣赏到原物和真迹为最大期盼；如果展出的是复制件或所谓的高仿件，则必须特别标明，尽管这必然会贬损展览的档次。在最能体现美术作品经济价值的拍卖行业，也是以“原件为王”，拍品一般都要附上权威鉴定机构的“验真”证明，否则根本上不了拍卖目录或拍不出高价。所以，无论从哪个方面讲，作品原件都是展览权架构中的核心概念和主要保护对象，因此也突显出准确建构美术作品原件的概念和创建美术作品原件认定规则的极端重要性。

2. 作品原件的唯一性和作为原件载体的物的唯一性的区别

在严格意义上，不存在完全相同的两个物，每个物都是独一无二的，承载作品的原件亦是如此。在数字化技术出现之前，对于美术作品而言可以将作品原件的唯一性和作品载体物的唯一性等同起来，对于摄影作品原件则需要另外讨论。数字化技术出现之后，只能笼统地说，作品原件的唯一性不是其载体物的唯一性，载体物的唯一性也不能决定作品原件的唯一性。对于数字化美术作品，如果使用同样的方法和材质，得到在普通人视觉上一般无二的两份及以上作品，如果均认定为作品原件，那么即可认为其唯一性被打破了；而作为承载作品的物，其相互之间仍然保持了各自的唯一性。

（二）几点重要考虑

从展览权的角度构建美术作品原件的概念，应当将以下几个方面纳入考量。

1. 美术作品的范围

《著作权法实施条例》第 4 条第 8 项规定：“美术作品，是指绘画、书法、雕塑等以线条、色彩或者其他方式构成的有审美意义的平面或者立体的造型艺术作品。”包括纯美术作品和实用美术作品。其中纯美术作品，是指仅能够供人们观赏的独立的艺术作品，比如油画、国画、版画、水彩画等。实用美术作品，是指将美术作品的内容与具有使用价值的物体相结合，物体借助于美术作品的艺术品位而兼具观赏价值和实用价值，比如陶瓷艺术等。〔23〕无需（美术）专业审视就可知道，我们通常认知的美术作品显然比上述规定要宽泛得多，各国立法例中美术作品的范围多数也比较宽泛。对于美术作品的法律界定和范围，既有国际公约的规定（《伯尔尼公约》第 2 条第 1 款），又有学者的细致分析，〔24〕均可借鉴。

实践中，符合大众认知和法律明确规定的美术作品较好判断，困难的是那些非典型的美术作品，比如名家的书信和手稿，还有音乐喷泉喷射效果的呈现和那些具有审美意义的建筑设计图、视觉效果图、手绘地图和模型等，也可以视为美术作品。随着《著作权法》的最新修订确立了“作品类型开放”的立法模式，还会出现更多不常见的美术作品类型，在事实上也增加了认定美术作品原件的难度。

2. 兼顾通过传统方法和通过数字化技术得到的美术作品原件

考察法律释义和学理研究，我国著作权法上美术作品原件的概念是建立在有体物基础之上

〔23〕 参见国务院法制办公室：《中华人民共和国著作权法注解与配套》，中国法制出版社 2017 年版，第 6 页。

〔24〕 参见郭玉军、陈云：《美术作品概念、成立要件及其范围的法律探讨》，载《湖北美术学院学报》2000 年第 2 期；王迁：《论平面美术作品著作权的保护范围——从“形象”与“图形”的区分视角》，载《法学》2020 年第 4 期；赵书波：《美术作品作者财产权益保护研究》，中国艺术研究院 2010 年博士学位论文，第 13－20 页。

的。比如，“美术作品原件，是指美术作品首次固定之有形载体”〔25〕；“作品原件，即作品的原始载体，是指作品在创作完成之时被固定其上的有形物质载体”〔26〕。《伯尔尼公约》第 2 条第 2 款也规定，未以某种物质形式固定下来的作品不受保护。对于用传统方法创作的美术作品，如此理解并无疑义。有疑义的是，如何确定通过数字化技术得到的美术作品的原件。比如，通过画图软件得到一幅美术作品，当作品完成时呈现在显示器上的画面是不是原件，这种呈现是否属于“固定”在载体上。〔27〕《美国版权法》第 101 条规定，用于固定作品的载体，应当具有“足够的长期性与稳定性”，以使作品在不短的一段时间内可以被感知、复制或以其他方式传播。考虑到显示画面的暂时性和该美术作品形成的电子文档在计算机内存上存储的暂时性，显示画面和内存模块似乎不能成为作品原件。由美术作品所形成的电子文档和存储该文档的计算机硬盘或光盘由于不具有我国著作权法所要求的“直接”可展览性，也不能当然地认定为原件。

版画作品和 3D 打印作品的原件也存在类似问题。版画的制作具有特殊性，先制版再印刷。先行制成的模版不是完整的版画作品，〔28〕不能视为版画作品的原件。如果套色印刷一张或若干张版画后，作者为了保证作品的稀缺性而毁掉模版，则印出来的版画作品（不论几张）即为原件似无疑义。如果保留模版，随时都可以印制出同样的版画作品，那么什么才是原件？或者说，在留存模版的情况下，版画作品是不是没有原件、只有复制件，或者印制出来的都是原件？

3. 突破美术作品原件必为物质实体的传统认识

目前理论和实务上均以物质实体为基础来认识美术作品原件，如“美术作品原件，是指美术作品首次固定之有形载体”〔29〕。然而，随着 2020 年 11 月《著作权法》的最新修订，这种传统认识正在发生变化。作为修订的一项重要内容，《著作权法实施条例》第 2 条的作品定义被修改、提升为《著作权法》第 3 条，〔30〕定义中的关键要素“能以某种有形形式复制”改成“能以一定形式表现”。对前者的重要理解之一就是作品可以以某种有形形式固定，而改为“能以一定形式表现”即放弃强调形式的有形，在一定程度上降低了对作品的固定性要求。

换言之，作品是不是必须固定下来，是不是必须以实体的方式存在，已经不是作品的构成要件了。那么，这种改变必然会影响到对美术作品原件的认识。早在二十多年前，日本著名学者就曾预言：“数字技术正在逐步的切断以往传统的著作物商业交易中所见到的无体物对有体物的寄生关系……著作物不再借用有体物的外衣而独立存在，我们面对的是一个全新的局面。”〔31〕《巴西著作权法》第 7 条也规定：“受保护的智力作品是指智力创作成果，而无论其表达形式如何，也无论其以任何有形的或无形的、现在已知的或将来可能开发的载体固定。”〔32〕所以，为了适应

〔25〕 前引〔7〕，李扬书，第 136 页。

〔26〕 曹新明：《作品原件所有人的告知义务研究——兼论〈著作权法〉第三次修订》，载《法治研究》2013 年第 11 期，第 42 页。

〔27〕 有学者认为，数字作品的物质载体是无形的电子脉冲。参见前引〔15〕，杨述兴文，第 41 页。

〔28〕 当然，具有审美意义的模版本身也是一种模型类的美术作品。

〔29〕 前引〔7〕，李扬书，第 136 页。

〔30〕 该条规定：“本法所称的作品，是指文学、艺术和科学领域内具有独创性并能以一定形式表现的智力成果，……”

〔31〕〔日〕北川善太郎：《网上信息、著作权与契约》，渠涛译，载《外国法译评》1998 年第 3 期，第 42 页。

〔32〕《十二国著作权法》，《十二国著作权法》翻译组译，清华大学出版社 2011 年版，第 9 页。

数字经济，有必要前瞻性地改造美术作品原件的传统认识。

4. 突破美术作品原件唯一的传统认识

在学理研究和审判实践中，普遍认为作品原件具有唯一性。前者如，“对于具体的作品而言，每个作品对应的原件具有唯一性”〔33〕；美术作品原件“有着复制件无可取代的价值和唯一性”〔34〕。后者如“成都市黑蚁设计有限公司与东宏实业（重庆）有限公司等著作权纠纷上诉案”，法院认为：“作品原件一旦形成，就具有唯一性，创作者永远也不可能再创作出一件与原件完全一样的美术作品。”〔35〕在用传统手法创作的年代，这种认识无疑是正确的，但是数字技术的发展已经颠覆了这种认识。比如，将电脑绘制的美术作品使用同样的打印机和纸张制作若干纸版，有可能都会被认为是原件。版画作品和 3D 打印作品的原件也是如此。版画的制作一般是先制版再印刷，制好的模版不是完整的版画作品，不能视为版画作品的原件。如果套色印刷一张或若干张版画后，作者为了保证作品的稀缺性而毁掉模版，则印出来的版画作品不论几张都是原件。对此，《法国知识产权法典》第 L.122—8 条第 2 款也规定，作品原件是指由艺术家亲自创作的作品，以及由艺术家亲自或在其指导下完成的限量版作品。所以，对于某些特定的美术作品和摄影作品，作品原件有可能不唯一。

必须指出，突破美术作品原件唯一的传统认识并非认为所有美术作品原件已经不再具备唯一性特征，而是表明唯一性已经不能作为一个能够涵盖所有美术作品原件的绝对特征，但不妨碍其仍可作为绝大多数传统美术作品甚至数字化美术作品的特征。比如近年来火爆全球的 NFT 数字艺术作品，在 NFT 技术的加持下也具备了唯一性。NFT 是在区块链的基础上发展起来的一种加密技术，通过区块链来记载上一个区块数字美术作品计算机文档的哈希值，其中就包括该作品每次流转的所有数据，并形成链接关系。任意一个区块发生人为的删改，后面相连的所有区块哈希值都会发生变化，于是链接上的每个环节都能发现数据被篡改，这样可以有效防止 NFT 数据被随意或恶意篡改。〔36〕同时，根据哈希算法，对数字艺术作品的任何修改都会产生不同的哈希值。因此，他人无法改变数字艺术作品以及链上哈希值而不被发现，也就保证了附有 NFT 数据的美术作品原件的唯一性。当然，这种唯一性并非通常意义上物理实体的唯一，也不是指在数字世界里只有一件数字美术作品，而是在无法篡改的技术保障下通过权属证明表现出来的“唯一”。

5. 坚守美术作品原件的不可替代性

美术作品原件的唯一性与其不可替代性紧密联系，著作权法强调保护美术作品原件的一个主要原因就是其具有不可替代性。如果作品原件可以被替代，变成对创作者、收藏者和观赏者可以旧去新来的物件，法律也就没有必要加强保护了。对于多数传统美术作品，作品原件唯一就意味着不可替代；而对于某些特定的美术作品和摄影作品，突破作品原件唯一的传统认识并非否认其不可替代性。实际上，不可替代性是确认美术、摄影作品原件的关键要素之一。有的学者认为，

〔33〕 袁博：《著作权法解读与应用》，知识产权出版社 2018 年版，第 123 页。

〔34〕 前引〔22〕，杨明文，第 261 页。

〔35〕 重庆市高级人民法院（2005）渝高法民终字第 76 号民事判决书。

〔36〕 参见王功明：《NFT 艺术品的价值分析和问题探讨》，载《中国美术》2021 年第 4 期。

可以将根据底片（胶卷拍照）或数码照片文档（数码拍照）洗印出来的照片均认定为摄影作品原件，〔37〕实际上是否定了原件的不可替代性。必须认识到，正是不可替代才使得美术作品原件稀缺而珍贵。

对于数字化美术作品，NFT 作品的每一个 TokenID（token identity document，代币唯一编码）都是独一无二、无法替代的。〔38〕即通过 NFT 技术，防止篡改和无法消除的权属凭证伴随并记录着该“唯一”美术作品的每一次流转，与其不可分离，在观念上、事实上和法律上都得到公认，保证了 NFT 美术作品的不可替代、不可互换。也许存在跟某件特定 NFT 美术作品数字化质量完全一样的其他 NFT 美术作品或非 NFT 美术作品，但是在 NFT 技术的规则之下，不存在相互替代的可能性。

6. 充实展览权的定义

现行著作权法赋予美术作品原件以“直接”可展览性，即现场直接展示作品原件本身。这对于展示作品载体即是展示作品的传统美术作品没有问题，但是却不能适用于以优盘、光盘为载体的数字化美术作品。当然，也可以将其打印出来展示，然而数字化美术作品的美感和价值更多的时候难以通过打印版展现出来。比如，三维美术作品的最佳展示方式是数字化的多角度展示，像素高度压缩的美术作品需要通过逐渐放大像素的方式来展现细微之美，还有动态的数字化美术作品也无法通过静置的方式展示。而且，同技术发展与时俱进的展览模式经常求新求变，那些比实物静置方式更活泼、效果更好的展览行为其实不受展览权的调整，比如常见的播放视频适用放映权，网上展示作品适用信息网络传播权。所以，有必要充实展览权的定义，参照《美国版权法》的“公开展示权”，明确规定既可以直接展示作品，也可以借助其他设备或方法间接展示作品。换言之，即赋予数字化美术作品以“间接”可展览性。

（三）构建美术作品原件的概念

虽然“作品原件”在我国著作权法中频频出现，却无相应定义。笔者认为，我国著作权法应当明确“美术作品原件”的法律含义。美术作品原件与复制件相对应，其概念必然要反映出二者的区别性，关键在于如何阐释“原”或“原件”的含义。笔者认为至少应当包括以下三个方面。

第一个方面是阐释为在时间上作品“首次”附着于载体或数字化作品的“首次”完成。前者是对传统上作品原件必为实体的理解，作者在载体物上完成作品之时，该载体物即成为原件；我国台湾地区“著作权法”第 3 条第 1 款第 14 项规定“原件指著作首次附着之物”，也是强调时间上的“首次”。后者是突破作品原件必为实体的认识，一幅数字化美术作品完成之时，即首次达到“能以一定形式表现”的法定要求，具备了成为作品原件的可能性。

第二个方面是阐释为作为复制件来源的原始件。原件先于复制件，复制件源于原件。复制可能是“二手”或“三手”，复制的维度也可能经历了二维和三维之间的转换，但是只有最原初的那件作品才是原件。

---

〔37〕 参见前引〔7〕，李扬书，第 137 页。

〔38〕 参见江哲丰、彭祝斌：《加密数字艺术产业发展过程中的监管逻辑——基于 NFT 艺术的快速传播与行业影响研究》，载《法学论坛》2021 年第 4 期；王铼、曹莹：《NFT 的境外法律监管》，载：http://glo.com.cn/Content/2021/05-24/1410013404.html，最后访问时间：2022 年 1 月 2 日。

如果原件已经遗失，作为原件的“一手”复制件，虽然是所有后续复制的来源，但显然不能认定为原件。此时就需要引入第三个方面，即“作者亲自创作完成”，这也正是作品创作的“原初”状态。其实，第一个方面和第三个方面只不过是对同一事实的不同表述而已，作者亲自创作作品过程的结束之时也就是作品“首次”固定或完成之时。参考《法国知识产权法典》第 L.122—8 条第 2 款，对于某些特定的作品，在作者指导下完成的限量版作品亦可认定为原件。比如，作者完成了模版的制作，然后亲自或指导他人印制出限量版画。

综上所述，可以将美术作品原件定义为：作者亲自创作且具有可展览性和不可替代性，并能以一定形式表现的美术作品。这是一个比较典型的“属＋种差”的逻辑定义，〔39〕可以从以下几个方面加以理解。

一是淡化了传统上强调美术作品在时间上的“首次”，将之隐含于“作者亲自创作”之中。凡是作者亲自创作的必然都是“首次”完成的作品，即便是作者反复创作主题、内容、布局、色彩等完全相同的作品，每一次创作都是单独创作，得到的每一件作品都是原件，而不是第一件作品或前一件作品的复制件。作者也许还会亲自复制，但既然不是创作，就只能是复制件。“作者亲自创作”实际上是所有作品原件的根本来源和本质属性。所以，如此定义表明了作品原件的本源，既强调了其在创作主体上的特定性，也涵摄了其在时间上的“首次”。

二是突出了美术作品原件相对于其他作品原件和美术作品复制件的差异性即“种差”。我国《著作权法》上的美术作品原件应当具有可展览性，这既是与其审美属性相辅相成的另一种本质属性，也是区别于其他作品原件的“种差”。在前文所述案例中，其他作品原件和美术作品原件的判决要旨截然不同，后者总是考虑是否侵犯了展览权。美术作品原件的不可替代性则是其区别于复制件的“种差”。作品复制件的可替代性决定了其不能像原件那样彰显作品与作者之间的人身联系，也无法达到作品原件的财产价值、收藏价值和观赏价值。如果说可展览性还可能会因为法律规定的不周延而产生不同理解（即“直接”和“间接”之分），那么不可替代性则是美术作品原件坚定不移的本质属性之一。

三是淡化了传统上认为作品原件必为实体的认识，既符合《著作权法》对作品定义的最新修订，也极大地扩展了作品原件的表现形式。《著作权法》的最新修订以“能以一定形式表现”替换作品定义中的“能以某种有形形式复制”，顺应了技术发展的时代趋势。可以预见，越来越多的数字化美术作品（包括将传统美术作品数字化）将放弃实体化的展示，而采用形式更加多样的数字展示方式。在美术作品原件的概念中使用“一定形式”的表述，既包括物质载体的形式，也囊括了现在及将来数字技术、智能技术所能带来的一切展示形式，大大提升了立法的前瞻性和应变性。

四、创建美术作品原件的认定规则

（一）美术作品原件的一般认定

以前述对美术作品原件概念的理解为基础，笔者认为，现实中美术作品原件已经具备了以下

〔39〕 这是一种常用的逻辑定义方法，被定义项由其属概念和其区别于其他种概念的种差组成。

几种可能性。

第一种可能是作品原件唯一，绝大多数通过纸笔或刻刀等传统手法创作的美术作品如是。作品原件就是美术作品首次固定于其上的物质载体，其与复制件在载体性质、大小比例甚至平面还是立体上可能相同，也可能不同。比如将画作、书法编印成集，将雕塑作品按比例缩小或印成图册。

第二种可能是存在若干份作品原件。比如，已经毁掉模版且印制质量、尺寸完全一样的若干张版画作品，均为原件。如果作者反复创作相同的作品，每一次都是独立的创作，得到的作品是相互独立的作品原件，而不是同一作品的若干份原件，更不是第一件作品的复制件。在这种情形下，原件的认定需要辅之以作者在原件上的签名、编号、盖章、水印等客观性证明。

第三种可能是一些特殊类型的作品原件附有存续期限。比如，为了举办大型活动用灯具或花盆摆设的艺术造型。在“自贡市公共交通总公司诉自贡市五星广告灯饰公司侵犯著作权案”中，法院就认定原告设计、制作的“希望之光”大型灯组属于《著作权法》所称的美术作品。〔40〕活动结束后拆除艺术装置，则美术作品原件灭失，其存续期限即为活动期间。再如雪雕作品、沙画作品也有一定的存续期限。还有判例将发型认定为立体美术作品，亦为附有存续期间的作品原件。

第四种可能是并非所有美术作品都有原件。比如，曾有判例将音乐喷泉喷射效果的呈现认定为美术作品。音乐喷泉喷射出来的艺术造型转瞬即逝，无法固定，但是满足了作品“能以一定形式表现”的法定要求。再如，烟花燃放和无人机编队形成的艺术造型也是类似的“瞬间载体”。《著作权法》的最新修订确立了“作品类型开放”的立法模式，未来也许会出现更多没有原件的美术作品类型。

（二）数字化美术作品原件的认定

首先，前文已述，存有电子文档的硬盘、光盘或优盘等存储器不具有“直接”可展览性和不可替代性，且该电子文档可以随时被删除，也不符合大众对作品原件的通常认知，不能作为作品原件。

其次，如同在画板上作画一样，数字化美术作品完成时呈现在显示器上的图片代表作品“首次”附着在物质载体上。但是，美术作品看似“固定”在屏幕上，其实只是暂存于计算机的内存中。而且，根据《美国版权法》第 101 条，用于固定作品的载体应当具有“足够的长期性与稳定性”，以使作品在不短的一段时间内可以被感知、复制或以其他方式传播。所以，这种短暂呈现的画面没有被真正固定下来，不具有稳定性，不能作为作品原件。

再次，如果坚持作品原件必为实体的传统认识，那么只能将打印出来的实体作品认定为原件。对照前述美术作品原件的概念，虽然其具备可展览性，但却不具备不可替代性，同样品质的作品制件可以反复制作。当然，作者可以通过签名、题词、盖章或印制时加入水印等技术手段将一张或若干张打印版特定化为不可替代的作品原件。但是，那些多维的、动态的或像素高度压缩的数字化美术作品只有通过数字化方式才能全方位展示出创作精髓。比如，2021 年 3 月，佳士得

〔40〕 参见四川省自贡市中级人民法院（1994）自民初字第 2 号民事判决书。

公司以 6934 万美元拍卖了一幅 NFT 数字化美术作品《Everydays-The First 5000 Days》，由作者从 2007 年 5 月以来 5000 个日夜所创作的数字化作品压缩而成，〔41〕其艺术价值不只是体现在由这些作品拼凑而成的整幅图片上，还包括可以被放大的每幅被压缩的作品。换言之，不能真正展现数字化美术作品美感的打印版“作品原件”颠覆了其原本应当具有的观赏性，有可能还贬低了作品的艺术价值。艺术家们肯定不愿看到自己精心制作的多维或动态数字化美术作品，只能展示其中静止不动甚至索然无味的一面。

最后，笔者认为，如果突破作品原件必为实体的认识，可以将数字化美术作品完成时的原始图片或其形成的电子文档（通常带有“.gif”或“.jpeg”等专用扩展名）认定为作品原件。此处的图片或电子文档指的是作者亲自创作完成的同一件作品的不同表现形式，均为同一事物，借助于看图软件即可将电子文档打开为图片。图片需要借助电子屏幕展示，电子文档需要借助看图软件和电子屏幕展示，均能间接地满足可展览性的要求，即具备“间接”可展览性。电子文档本身附有权利管理信息，〔42〕可以被特定化为不可替代物，作者还可以通过技术措施防止他人未经许可浏览、欣赏和复制作品。《著作权法》的最新修订不仅将原来规定于《信息网络传播权保护条例》的权利管理信息和技术措施提档升级，还正式纳入作品登记制度，亦可为数字化美术作品原件的认定提供公信力极强的证明。

现实中的主要问题在于权利管理信息或技术措施极易被他人攻破，安全性比较低，特别是价值越高的作品越容易遭到攻击；一旦权利管理信息被篡改或删除，数字化美术作品原件就失去不可替代性，和其他拷贝文档混同为彼此没有差别的复制件。

然而，NFT 技术的出现提出了一个有希望的解决途径，在数字化美术作品的真伪鉴定、确认所有权、打击盗版和保护、管理版权等方面都产生了积极的影响。〔43〕2021 年 3 月有两则消息引人注目：一是推特（Twitter）联合创始人、首席执行官杰克·多西（Jack Dorsey），以 291 万美元拍卖了其 2006 年 3 月在 Twitter 上发表的第一条推文；〔44〕二是佳士得公司以 6934 万美元拍卖 NFT 作品《Everydays-The First 5000 Days》〔45〕。两件数字化作品都采用 NFT 技术予以特定化，保证了买家与拍品之间唯一的对应关系。在 NFT 作品拍卖中，买卖的其实是一种所有权凭证。NFT 通过一种技术方法来证明对数字艺术作品享有相应权利，并由区块链技术确保无法篡改，成为牢不可破的权利管理信息。当作者将其数字化美术作品的哈希值上传区块链并经由 NFT 技术特定化后就成为作品原件，其后该原件的每一次流转都被记录下来并不可篡改，满足了唯一性和不可替代性的要求，亦可借助电子屏幕进行展示，具备了可以作为作品原件的基本特征。因此，通过 NFT 技术认定数字化美术作品原件在技术上可行，并已投入应用，国内外也已

〔41〕 参见司林威：《NFT 玩家，谁都不曾拥有，我们只是过客》，载 https://baijiahao.baidu.com/s?id=1695901624768440859&wfr=spider&for=pc，最后访问时间：2021 年 3 月 31 日。

〔42〕 根据《信息网络传播权保护条例》第 26 条，“权利管理信息”是指说明作品及其作者、表演及其表演者、录音录像制品及其制作者的信息，作品、表演、录音录像制品权利人的信息和使用条件的信息，以及表示上述信息的数字或者代码。

〔43〕 参见刘双舟、郭志伟：《论非同质化代币对数字艺术版权管理与保护的影响》，载《中国美术》2021 年第 4 期。

〔44〕 参见揭书宜：《卖出 290 万美元！推特 CEO 首条推文以 NFT 资产卖了》，载 https://www.thepaper.cn/newsDetail_forward_11836514，最后访问时间：2021 年 3 月 23 日。

〔45〕 参见前引〔41〕。

经形成了一个创作和买卖、收藏 NFT 作品的新业态。

（三）美术作品的复制件

与作品原件相比，美术作品复制件的特殊问题在于，与原件不同维度的复制件是否仍是展览权意义上的作品复制件。复制行为本身有广狭之分，狭义的复制仅指同一维度的平面到平面、立体到立体，广义的复制还包括从平面到立体、立体到平面的维度改变。

对此，有肯定和否定两种见解。否定见解采狭义复制论，认为改变了作品原件维度的复制件不是展览权意义上的作品复制件。在“范英海、李先飞诉北京市京沪不锈钢制品厂著作权纠纷案”中，法院认为：“对于包括雕塑作品在内的美术作品，其复制件应指由对该作品的复制行为所产生的与该作品完全相同或者相近似的作品。由于被告展览的涉案不锈钢雕塑作品构成了对原告雕塑作品《韵》的剽窃，该剽窃作品应属原告雕塑作品《韵》的复制件。”〔46〕肯定见解采广义复制论，认为与作品原件维度不同的复制件仍是展览权意义上的作品复制件。比如，在“广东原创动力文化传播有限公司（以下简称‘原创公司’）诉群光实业（武汉）有限公司（以下简称‘群光公司’）著作权纠纷案”中，群光公司购买了与原创公司美术作品美羊羊、喜羊羊、灰太狼在视觉上无明显差异的服装道具，派员工穿戴该卡通服装道具装扮成卡通角色在其周年庆活动上宣传造势，并与现场人群交流互动。其中，涉案侵权物品即为源于平面美术作品的立体卡通服装道具。法院认为：“被告的行为使原告美术作品美羊羊、喜羊羊、灰太狼的立体复制件向不特定公众展示，虽属于非典型的公开陈列美术作品的行为，但仍侵犯了原告对以上美术作品享有的展览权。”〔47〕

我国《著作权法》采用狭义复制的概念即否定见解，然而从著作权法鼓励和保护作品及其创作的目的出发，采肯定见解即广义复制的概念更为合理。盖因著作权法保护的是作品而非作品载体，如果将改变作品原件维度的复制件放任于法律调整之外，显然不利于维护著作权人的利益，也是一种纵容侵权的做法。

根据上述认定规则，经由 NFT 证明或其他类似证明的数字化美术作品的图片或电子文档是原件，没有相应证明和已经实体化的作品都是复制件；进而言之，对于数字化美术作品，其复制件具有数字化和实体化两种可能的属性。将实体化的美术作品原件进行数字化复制，得到的数字化作品也可称为复制件。这样无论通过什么方式创作作品，均突破了作品复制件必为实体的传统认识，和确定作品原件的规则保持了一致。《著作权法》的最新修订修改了第 10 条关于复制权的定义，专门将“数字化”的复制加入其中。有学者认为：“这一修改只是对理论和实务中的共识以立法形式加以体现，是对已有做法的确认，而不是创设新的规则。”〔48〕所以，改变美术作品原件和复制件必为实体的认识，在理论、实务和法律依据上都已具备了一定的基础。

五、结　语

展览权虽然在著作财产权中并不起眼，但却是文博事业存在和发展的重要基石。作为展览权

〔46〕 北京市第二中级人民法院（2002）二中民初字第 8042 号民事判决书。

〔47〕 湖北省武汉市中级人民法院（2010）武知初字第 66 号民事判决书。

〔48〕 王迁：《〈著作权法〉修改：关键条款的解读与分析》（上），载《知识产权》2021 年第 1 期，第 24 页。

的核心概念和拍卖场的竞逐对象，美术作品原件的重要性毋庸置疑。我们应当从实践出发，回应新技术、新业态提出的新挑战，正确理解和认识美术作品原件的概念，突破作品必有原件、作品原件唯一和作品原件必为实体的传统认识，顺应数字经济时代的发展趋势，构建出认定美术作品原件特别是数字化美术作品原件的新规则。

Abstract：The original copy of art works is the core concept of the display right in China's Copyright Law，but it has not received due attention. Facing the new challenges posed by new technologies and new business forms，regardless of traditional art works or digital art works，there is a confusion about how to understand the original copy of art works and how to identify the original copy of art works. In this regard，it is necessary to break through the traditional understanding in Copyright Law that art works must have the original copies，that the original copies of art works must be unique and that the original copies must be entities. Complying with the requirements of technological development，we should firmly grasp the two key characteristics of exhibitability and irreplaceable to construct the concept of the original copy of art works and create the general rules for identifying the original copy of art works. For digital art works，on the premise of meeting the "indirect" exhibitability，the electronic documents formed when the digital art works are completed can be recognized as the original copies with the help of NFT technology.

Key Words：art works，original copy，the display right，non-fungible token

（责任编辑：张金平　赵建蕊）

财经法学 No. 4，2022
pp. 67 - 82

算法解释在民法中的体系定位与类型区分

胡巧莉　刘征峰*

内容提要：从民法视角观察，个人信息应作为法益保护。针对自动化决策的算法解释实际上是人格权衍生的非独立请求权，无需单独创设一项算法解释权。算法解释在合同领域中可被纳入保护义务的范畴，在侵权领域中则具有过错评价的功能，当个人信息处理者无法解释或拒绝解释时，可推定其存在过错。为保护个人信息处理者的商业秘密，减轻其解释负担，《个人信息保护法》第24条第3款所规定的算法解释应区分为事前解释与事后解释两种类型，两者在要件构造与解释程度上存在区别。事前解释应限定于“可能产生重大影响”的敏感个人信息处理场合，事后解释则发生在“对个人权益已经产生重大影响”的自动化决策场合。事前解释义务的程度应低于事后解释义务，二者分别对应对系统功能的抽象解释和对具体决策的详细解释。因重大影响产生实际损害后，个人信息主体可通过主张违约或侵权损害赔偿责任实现救济。对事前解释义务的意定免除若违反《民法典》第497条或第506条应为无效，但事后解释义务及其衍生的损害赔偿请求权可被免除。

关键词：算法解释　个人信息权益　自动化决策　重大影响

在利用个人信息的自动化决策场合，难免在信息剖析时因“歧视性”因素而作出对个人存在重大影响或产生法律效力的决策。〔1〕规制算法的方式是将存在实质性歧视、隐私风险以及其他重大影响的决策结果纳入法律调整的范围，如个人信息主体可要求作出“算法解释”。〔2〕域外法上对“算法解释”的讨论聚焦于“算法解释（权）”的规范依据与权利性质。〔3〕欧盟以《一般数据

* 胡巧莉，中南财经政法大学法学院硕士研究生；刘征峰，中南财经政法大学法学院副教授。

〔1〕 See Bart Custers et al. ed., *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases*, Springer, 2012, p. 138.

〔2〕 参见郑智航、徐昭曦：《大数据时代算法歧视的法律规制与司法审查———以美国法律实践为例》，载《比较法研究》2019年第4期。

〔3〕 See Sandra Wachter et al., Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 *International Data Privacy Law* 76, 77 - 81 (2017); Paul Vogel, A “Right to Explanation” for Algorithmic Decisions?, in Amedeo Santosuosso, Giulia Pinotti ed., *Data-Driven Decision Making. Law, Ethics, Robotics, Health*, Pavia University Press, 2020, pp. 49 - 52.

保护条例》（下文简称 GDPR）第 22 条和序言第 71 条为依据，保障个人有权不受对其产生法律效力或者类似重大影响的自动化决策之约束。为维护市场交易语境下的数据公平（或称免于受欺诈或不公平对待），美国以《信贷机会均等法》（The Equal Credit Opportunity Act）和《公平信用报告法》（Fair Credit Reporting Act）作为“算法解释（权）”的主要规范依据，专门规定了贷方需就不利的算法评分向消费者解释的义务。

我国立法文本中未出现“算法解释（权）”这样的表达，但根据《个人信息保护法》第 24 条第 3 款的规定，个人信息主体有权要求个人信息处理者说明对其权益有重大影响的自动化决策，并享有相应的拒绝权。值得探讨的是，该款规定隐含的“算法解释”在民法上究竟属于何种性质，又可产生何种法律效果。我国学界对“算法解释”是否为一项独立的民事权利存在争论，肯定者认为个体赋权式的治理模式可为个人信息提供更强保护，〔4〕并由此形成完整的个人信息权利体系。否定者则认为个人信息仅需作为利益保护，算法解释的功能可被现有的法律制度涵盖，创设算法解释权易形成保护功能的堆叠。〔5〕两种相反的观点虽各有理由，但未能就民法体系中如何理解算法解释作出圆满的回应。无论采何种规范模式，核心是如何在主观权利体系中厘清“算法解释”的保护目的与体系价值。

本文以利用个人信息的自动化决策为研究对象，首先从“算法解释”保护的个人信息权益的法律评价出发，判断算法解释能否被人格权中的个人信息保护（《民法典》第 1032 条至第 1039 条）、消费者知情权（《消费者权益保护法》第 8 条、第 14 条以及《个人信息保护法》第 44 条）、合同保护义务、侵权责任等民法保护模式的规范功能所涵括，明晰其性质与定位。在此基础上，尝试在民法体系中对算法解释进行类型区分，重点分析类型区分的实益以及不同类型算法解释的规范构造。

一、人格权体系中的算法解释

《个人信息保护法》第 24 条规定了利用个人信息的自动化决策和相应的“算法解释”义务。算法解释作为保护个人信息权益的方式，其体系定位与规范性质尚未明确，关键在于目前的民法体系中是否已经存在可以承载“算法解释”的规范制度。因此，首先，需要先明确个人信息权益的性质，再判断算法解释的体系位置是处于“个人信息保护体系”还是人格权保护体系，其性质为独立权利还是请求权。其次，基于算法解释的规范目的，自动化决策对个人权益的重大影响产生的时间不同，需区分不同的算法解释类型。

（一）作为非独立请求权的算法解释

《民法典》规定自然人的个人信息受法律保护，列明了个人信息处理中需遵循的原则和违反相应义务时需承担的责任。《个人信息保护法》对个人信息保护作出了更为详尽的规定，但均未

〔4〕 参见张凌寒：《商业自动化决策的算法解释权研究》，载《法律科学（西北政法大学学报）》2018 年第 3 期；张恩典：《大数据时代的算法解释权：背景、逻辑与构造》，载《法学论坛》2019 年第 4 期；解正山：《算法决策规制——以算法“解释权”为中心》，载《现代法学》2020 年第 1 期。

〔5〕 参见贾章范：《论算法解释权不是一项法律权利——兼评〈个人信息保护法（草案）〉第二十五条》，载《电子知识产权》2020 年第 12 期；辛巧巧：《算法解释权质疑》，载《求是学刊》2021 年第 3 期。

言明“个人信息权”的存在，仅出现“个人信息权益”的表达。个人信息属于人格要素，与人格权的保护内容存在交叉，若重复性地创设独立的“个人信息权”，则会与人格权的保护体系产生叠合。〔6〕立法政策对个人信息保护采行为规制模式，正是由于个人信息权益尚未达致“权利的分配密度”（Zuweisungsdichte）。〔7〕行为规制模式将个人信息视为一项法益，规制信息处理行为，既可避免权利泛化，亦可缓解与个人信息利用与保护之间的紧张关系。〔8〕因此，个人信息法益可置于人格权规范体系下予以保护，尽管《个人信息保护法》第四章“个人在个人信息处理活动中的权利”中使用了“权利”，但其仅为技术意义上的表达，与《民法典》第五章“民事权利”中具体列举的生命权、身体权等权利的性质并不相同，将其理解为保护个人信息法益的请求权更为适宜。

在明确了个人信息权益属于人格权保护体系的法益后，作为其保护方式的“算法解释”，亦应当被置于人格权保护体系的范畴进行性质界定。对于“算法解释”的关键争议在于《个人信息保护法》第 24 条第 3 款是否创设了“算法解释权”。支持的观点认为目前的法律资源不敷适用，应配置独立的算法解释权，用以平衡自动化决策使用者与相对人不对称的权力关系。〔9〕只有通过赋权才能增强算法透明性，以破解“算法黑箱”的方式达到提高算法可责性的目的。〔10〕否定的观点认为算法解释的功能可通过其他规制手段实现，〔11〕创设权利的救济效果有限，会对商业秘密、国家利益和市场竞争秩序造成不良影响，徒增裁判成本。〔12〕深思之，支持算法解释“权利化”的观点未从民法体系的视角去观察算法解释的定位。算法解释所保护的法益可以被人格权规范体系所涵盖，在合同与侵权领域表现为不同的保护手段与规范功能。至于商业秘密，其仅构成对算法解释说明义务的限制，不能绝对地拒绝算法解释请求权的适用。〔13〕

域外法上，学者们以 GDPR 第 22 条及序言第 71 条为核心对算法解释的规范模式展开了讨论。有观点认为即便序言在欧盟法律下并不具有拘束力，但为了引导数据主体依据 GDPR 行使权利，至少应保障其从功能角度获得解释的利益。〔14〕相反观点则认为 GDPR 第 22 条并未明文规定“算法解释权”，序言第 71 条虽提及“算法解释权”（the right to obtain an explanation of the decision），但其未处于正式文本中，不可创设权利类型。〔15〕亦有观点主张“算法解释权”可能引发新的“透明性谬误”，通过被遗忘权、数据可携带权、隐私保护等即可使算法更加注重

〔6〕 参见郑晓剑：《个人信息的民法定位及保护模式》，载《法学》2021 年第 3 期；程啸：《论我国民法典中个人信息权益的性质》，载《政治与法律》2020 年第 8 期。

〔7〕 Vgl. Schwab/Löhnig，Einführung in das Zivilrecht，20. Aufl.，2016，Rdn. 263.

〔8〕 参见黄薇主编：《中华人民共和国民法典人格权编释义》，法律出版社 2020 年版，第 196 页。

〔9〕 参见前引〔4〕，张凌寒文；前引〔4〕，解正山文。

〔10〕 参见姜野、李拥军：《破解算法黑箱：算法解释权的功能证成与适用路径——以社会信用体系建设为场景》，载《福建师范大学学报（哲学社会科学版）》2019 年第 4 期；许可、朱悦：《算法解释权：科技与法律的双重视角》，载《苏州大学学报（哲学社会科学版）》2020 年第 2 期。

〔11〕 参见前引〔5〕，辛巧巧文。

〔12〕 参见前引〔5〕，贾章范文；李天助：《算法解释权检视——对属性、构造及本土化的再思》，载《贵州师范大学学报（社会科学版）》2021 年第 5 期。

〔13〕 参见吕炳斌：《论个人信息处理者的算法说明义务》，载《现代法学》2021 年第 4 期。

〔14〕 See Bryan Casey et al.，Rethinking Explainable Machines：The GDPR's “Right to Explanation” Debate and the Rise of Algorithmic Audits in Enterprise，34 *Berkeley Technology Law* 143，159－161（2019）.

〔15〕 参见前引〔3〕，Sandra Wachter 等文，第 79－80 页。

个体利益保护。〔16〕不同成员国对算法解释的规范模式并未与 GDPR 完全保持一致。德国、比利时并未肯认 GDPR 序言第 71 条所提及的“算法解释权”。〔17〕可能的原因在于，基于算法自动化决策所作出的歧视性结果可由其他法律规范进行规制。如德国《一般平等待遇法》不仅将损害赔偿作为救济方式，而且将救济方式扩展至可能对契约自由作根本性否定的强制缔约。〔18〕“如果歧视行为表现为拒绝订立合同，在只有通过订立合同才能排除妨碍的情况下，排除妨碍的外延中实际上包含了强制缔约这一方式。”〔19〕在英国与爱尔兰的《数据保护法》中，虽不能直接看出“算法解释权”，但其均要求数据控制者阐明算法分析的过程。〔20〕法国和匈牙利的相关法令将“算法解释权”纳入了规范范畴，只是在行使的具体要求上略有不同。〔21〕甚者，意大利最高上诉法院在判决中直接将“算法是否透明”作为个人信息处理中的“个人同意”是否有效的关键因素。若算法不透明则个人信息主体作出的“同意”归于无效，对利用算法进行自动化决策的手段进行严格规制。〔22〕

还有学者倾向于将概念限缩，不称其为“解释权”（right to explanation）而称其为“知情权”（right to be informed），认为知情内容包括算法系统功能与具体的自动化决策。〔23〕但知情权对应的是个人信息处理者的事前告知义务，披露的时间为收集信息时、处理个人信息前，不包括处理个人信息并作出决策后的情形。〔24〕在内容上，知情权旨在披露个人信息处理的主体、目的、内容、方式以及享有的访问权等权利，〔25〕不包括对具体自动化决策结果的解释。我国《个人信息保护法》第 44 条规定个人对其个人信息的处理享有知情权，并未言明知情的具体内容。第 17 条对告知义务内容的规定亦不包含针对个人的具体自动化决策。

因此，算法解释并不等同于算法透明原则项下的知情权。知情权的内容较算法解释更为狭窄，不要求“重大影响”作为要件，亦不包含复杂的事后解释类型。若不对事前与事后进行区分，统一以知情权保护，将会忽略对个人信息处理者商业秘密的保护和解释负担的关注。在规范效果上，算法解释不仅具备与告知义务类似的事前防御性效果，还有事后救济的功能，具体表现为合同领域中义务不履行责任的判断和侵权责任领域中过错的评价。无论是《消费者权益保护法》中的消费者知情权，还是《个人信息保护法》中的个人信息主体的知情权，均无法完全囊括

〔16〕 See Lilian Edwards, Michael Veale, Slave to the Algorithm: Why a Right to An Explanation Is Probably Not the Remedy You Are Looking for, 16 *Duke Law & Technology Review* 18, 19 - 20 (2017 - 2018).

〔17〕 See Gianclaudio Malgieri, Automated Decision-making in the EU Member States: The Right to Explanation and other “Suitable Safeguards” in the National Legislations, 35 *Computer Law & Security Review* 1, 8 - 13 (2019).

〔18〕 参见刘征峰：《从“反歧视原则”进入民事交易关系观察当代民法理念的革新》，载《法制与社会发展》2017 年第 1 期。

〔19〕 Haberl, Antidiskriminierungsrecht und Sanktionenssystem: Die Konkretisierung gemeinschaftsrechtlicher Mindestvorgaben, GPR 6 (2009), 202, 202 - 209.

〔20〕 See UK Data Protection Act 2018, Chapter 2, Section 14; Irish Data Protection Act 2018, Part 3, Chapter 3, Article 57.

〔21〕 参见前引〔17〕，Gianclaudio Malgieri 文，第 21 - 22 页。

〔22〕 See Giorgia Bincoletto, Italy Supreme Court of Cassation on Automated Decision Making: Invalid Consent if an Algorithm is Not Transparent, 7 *European Data Protection Law Review* 248, 248 - 249 (2021).

〔23〕 参见前引〔14〕，Bryan Casey 等文，第 161 页。

〔24〕 See Isak Mendoza, Lee A. Bygrave, The Right Not to Be Subject to Automated Decisions Based on Profiling, in Synodinou et al. ed., *EU Internet Law: Regulation and Enforcement*, Springer, 2017, p. 93.

〔25〕 See GDPR Article 13、Article 14；我国《个人信息保护法》第 17 条。

算法解释的规范功能。

综上所述，判断“算法解释（权）”是否存在，不应拘泥于立法文本的形式表达，应当充分结合背后的规范目的和价值考量。从《民法典》所采的立场来看，作为一般人格权条款的第990条第2款以“其他人格权益”保护一般人格权，与该条第1款所规定的具体人格权相区分。〔26〕个人信息保护的诸多内涵可被纳入具体人格权与一般人格权益的保护范畴。因此，在不存在独立的个人信息权的前提下，算法解释作为保护个人信息权益的方式，既不是作为个人信息权的权能，也不是作为独立的算法解释权，其民法性质为保护个人信息法益的非独立请求权。〔27〕

进一步而言，算法解释是依附于人格权保护体系、为实现人格利益保护而服务的非独立请求权。《个人信息保护法》第24条第3款和第48条规定的解释义务以及第44条所规定的“知情权”存在保护内容上的重合之处，均构成个人信息主体在个人信息处理中要求事前知情或者事后解释的权益保护手段。对于《个人信息保护法》与《民法典》之间的适用关系，合理的模式应为《民法典》人格权编仅对个人信息保护作出原则性和转介性的规定，《个人信息保护法》对具体问题作出更为细致的规范。在《个人信息保护法》中没有明文规定时，才可适用《民法典》中的一般条款。〔28〕

（二）非独立请求权性质下的类型区分实益

正如前文所言，若不对算法解释进行事前事后的区分，可能导致其与知情权的混淆和对事后救济功能的忽视。个人信息属于人格要素，而保护人格权的方式在事前和事后有所区别，损害产生的事前表现为防御型请求权，损害产生的事后表现为救济型请求权。因此，值得探讨的是：算法解释作为人格权保护项下的非独立请求权，是否应参照人格权保护方式因事前事后的差异而区分不同的类型。

GDPR未对算法解释的性质属于事前解释还是事后解释作出明确规定。〔29〕事前解释发生于算法提供者基于用户同意开始收集个人信息后、自动化决策作出前，决策系统的规则设计可能对个人信息主体权益产生重大影响。事前解释提供的信息为系统功能，例如可能被考虑的数据类型及特征或决策树的分级标准等，未具体到个人信息主体。〔30〕事后解释则发生在自动化决策已经作出，且对个人信息主体的个人权益产生了重大影响的情形。事后解释的内容既包括系统功能也包括针对个人的具体决策，如某一特定主体被采纳的信息类型、个案中纳入自动化决策的因素和权重、对权益产生的重大影响等。〔31〕

与合同法上的保护义务以及侵权责任领域的交往安全义务相类似，只有当个人信息主体与个人信息处理者进入到一定程度的特别结合关系中，才可对其施加解释义务的负担，不可在尚未开

〔26〕 参见朱晓峰：《论一般人格权条款与具体人格权条款的规范适用关系》，载《比较法研究》2021年第3期。

〔27〕“请求权有独立请求权与非独立请求权之分，独立的请求权不依赖于其他权利而独自存在，本身即属于一种权利，而非独立请求权则是为实现其他的权利服务的。”参见〔德〕卡尔·拉伦茨：《德国民法通论》（上册），王晓晔等译，法律出版社2013年版，第325页。

〔28〕 参见王苑：《个人信息保护在民法中的表达——兼论民法与个人信息保护法之关系》，载《华东政法大学学报》2021年第2期；石佳友：《个人信息保护的私法维度——兼论〈民法典〉与〈个人信息保护法〉的关系》，载《比较法研究》2021年第5期。

〔29〕 参见前引〔3〕，Sandra Wachter等文，第82页。

〔30〕 参见前引〔3〕，Sandra Wachter等文，第78页。

〔31〕 参见前引〔17〕，Gianclaudio Malgieri文，第22－23页。

始收集个人信息时即要求作出事前解释。但我国《个人信息保护法》第 24 条第 3 款忽略了事前解释与事后解释在保护目的和解释内容上的区别。本文认为，应作事前解释和事后解释的类型区分，区分的实益如下：

首先，事前解释的功能无法被《个人信息保护法》第 17 条的事前告知义务所涵盖，该条第 1 款第 2 项规定，个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人信息主体告知个人信息的处理目的、处理方式、处理的个人信息种类、保存期限。其中的处理方式仅意味着选择人为还是自动化决策，〔32〕并不要求具体解释算法系统功能以及算法运行规则。《个人信息保护法》第 48 条规定个人信息主体可要求个人信息处理者解释说明的“个人信息处理规则”，与第 17 条的“处理的方式”亦不相同。

有学者提出“算法说明义务”这一概念，认为从告知义务中可推导出“算法说明义务”，其适用于算法决策的全过程，以避免陷入算法解释是否为独立权利类型的争议。算法解释仅包括自动化决策已经对个人权益产生重大影响的事后解释，而“算法说明义务”则不拘泥于“重大影响”这一条件。〔33〕该观点存在以下可供商榷之处：第一，“算法说明义务”是一个较为模糊的概念，其简单地将“告知义务”与“算法说明义务”等同，但无论是《个人信息保护法》第 7 条、第 14 条还是第 17 条均无法解释“算法说明义务”的具体内涵。第二，通过模糊概念规避算法解释的性质分析存在不妥。如前文所述，算法解释的性质应为人格权保护体系中的非独立请求权。《个人信息保护法》第 24 条第 3 款不仅包括事后解释，亦包括自动化决策作出前的事前解释。事前解释与事后解释在适用要件上有所区别，前者仅要求“可能的重大影响”，后者要求“已经产生重大影响”。第三，前文已述，《个人信息保护法》第 17 条规定的告知义务仅为事前告知义务，若将“告知义务”与“算法说明义务”等同，则“算法说明义务”无法包含事后说明的类型。第四，若“算法说明义务”无需要求“重大影响”这一要件，会过度增加个人信息处理者的解释负担，不利于个人信息的流通。因此，通过“算法说明义务”无法否定算法解释存在事前解释和事后解释两种类型。

其次，事前解释注重防御性的保护，目的在于避免抽象的重大影响转化为针对个人的重大影响；事后解释则注重对已经发生的重大影响作出解释，并在重大影响转化为损害后对义务违反及过错要件进行评价。事前解释作为防御性请求权，可以为损害实际产生前的个人信息主体提供预防性的保护，尤其是以敏感个人信息为对象的处理行为。这与《民法典》第 997 条规定的防御性请求权的规范功能相似。该条的根本目的在于为人格权保护提供高效、便捷的预防性保护措施。〔34〕对于自动化决策中个人权益的保护亦应如此。虽然此时损害尚未发生，但损害赔偿带来的负担不仅仅发生在具体加害人与受害人之间，还会造成额外的社会支出，预防损害能够以最低成本产生最大收益。〔35〕不过，事前解释的适用场景需作限缩，否则会对个人信息处理者造成过

〔32〕 参见程啸：《个人信息保护法理解与适用》，中国法制出版社 2021 年版，第 179 页。

〔33〕 参见前引〔13〕，吕炳斌文。

〔34〕 参见程啸：《论我国民法典中的人格权禁令制度》，载《比较法研究》2021 年第 3 期。

〔35〕 参见朱岩：《侵权责任法通论·总论》，法律出版社 2011 年版，第 107 页；〔奥〕海尔姆特·库齐奥：《侵权责任法的基本问题（第一卷）：德语国家的视角》，朱岩译，北京大学出版社 2017 年版，第 78－80 页。

重的解释负担。

再者，区分事前解释与事后解释更有利于实现对商业秘密的保护。在自动化决策作出前，个人权益尚未受到重大影响，应基于比例原则承认商业秘密对解释请求权的一般性抗辩。“合法、正当、必要原则”已成为个人信息处理的基本原则（《个人信息保护法》第5条），是比例原则在民法中的体现，有益于弥补数字时代意思自治与契约自由的缺陷。〔36〕比例原则的适用不应局限于个人信息处理者的处理行为，还应包括对个人信息主体算法解释请求权的限制。例如，作为框架权的一般人格权的效力弱于具体人格权，只有通过利益权衡，才能认定是否存在侵害这些权益的行为。在进行利益权衡时，必须考虑到其他人与此相冲突的权益。〔37〕基于人格权所衍生的非独立请求权更应如此，当事前解释与他人的商业秘密产生冲突时，由于此时对个人信息主体权益的重大影响尚未实际产生，故个人信息处理者的商业秘密应优先受到保护。

正如GDPR序言第63条所指明的，个人信息权利的行使不应对其他主体的合法权益产生不利影响，尤其是商业秘密、知识产权以及软件版权。〔38〕实践中，多数个人信息处理者在拒绝作出解释时给出的理由为“保护商业秘密”。如在“卢米斯案”中，上诉法院因“商业秘密保护”而拒绝了被告所提出的“打开再犯风险评估算法”的请求。〔39〕在“SCHUFA案”中，当事人因较低的自动化信贷评分而失去了借贷机会，但其在申请评估公司公开计算评分的算法规则时，同样被法院以保护商业秘密的理由而驳回。〔40〕算法本身具有客观性，且往往蕴含着商业秘密，这已成为增强算法问责制和透明度的主要障碍之一。〔41〕有观点认为，只有在算法解释涉及公共利益的情形下才可考虑进行公开。〔42〕

我国《个人信息保护法》第48条未对解释说明的限度、个人信息处理者的抗辩事由作出规范。在实践中，如果缺乏法律的明确规定，平衡算法解释与商业秘密将会面临较大的困境。〔43〕商业秘密保护有效地在算法中创造了一种不需要公开的财产权益，但这并非意味着只要进行算法解释就会不利于商业秘密的保护。首先，算法解释的内容并非均属于商业秘密的范畴。复杂的代码与运算模型对于非专业人员而言并无解释的实质效果，只有将算法解释与具体的决策结果相联系，才能够达到个人信息主体主张解释的目的。其次，算法解释所寻求的是“有法律意义的信息”，通过对解释对象和解释内容的限制可以规避侵害商业秘密的风险。在解释对象上，可针对某些特定群体进行小范围的公开解释。在解释内容上，无需对核心算法进行公开解释，但至少应当公开影响算法决策过程的决定性因素及一般操作模式。〔44〕在解释条件上，限于法律明确规定

〔36〕 参见刘权：《论个人信息处理的合法、正当、必要原则》，载《法学家》2021年第5期。

〔37〕 参见〔德〕迪特尔·梅迪库斯：《德国民法总论》，邵建东译，法律出版社2013年版，第107页。

〔38〕 See GDPR Recital 63 sentence 5.

〔39〕 See State v. Loomis. 881 N. W. 2d 749 (Wis. 2016).

〔40〕 Vgl. BGHZ 200, 38.

〔41〕 See Sonia K. Katyal, Private Accountability in the Age of Artificial Intelligence, 66 *U. C. L. A. Law Review* 54, 54－59 (2019).

〔42〕 See Campbell v Frisbee [2002] EMLR 31; Guido Noto La Diega, Against the Dehumanisation of Decision-Making-Algorithmic Decisions at The Crossroads of Intellectual Property, Data Protection, and Freedom of Information, 9 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 3, 13 (2018).

〔43〕 See Gianclaudio Malgieri, Trade Secrets v Personal Data: A Possible Solution for Balancing Rights, 6 *International Data Privacy Law* 102, 102－106 (2016)；前引〔42〕，Guido Noto La Diega文，第14－18页。

〔44〕 参见前引〔3〕，Paul Vogel文，第54－55页。

的情形或者仅在个案中向单个数据主体披露。〔45〕因此，将可能涉及商业秘密的解释内容限制在事后解释的范畴则可避免对个人信息处理者商业秘密的过度妨害。

综上所述，应以对个人权益的重大影响或损害实际发生的时间为节点，对算法解释的类型作出区分，分为收集信息后决策作出前可能产生重大影响的事前解释与决策作出后并产生重大影响的事后解释两种类型。类似于合同缔结前后双方当事人所承担的保护义务内容与程度的差异，事前解释的义务低于事后解释，以平衡个人信息主体的合法权益与个人信息处理者的商业秘密保护等利益。

二、事前的算法解释与基于同意的义务免除

根据《个人信息保护法》第 24 条第 3 款的规定，算法解释需遵循的规范要件有二：第一，自动化决策。《个人信息保护法》第 24 条第 3 款中“拒绝”所指向的是“仅通过自动化决策的方式作出决定”，不包括掺杂人工干预的自动化决策结果。第二，该决策对个人权益有重大影响。个人权益并不限于个人信息权益，亦包括《民法典》总则编第 5 章所规定的其他民事权利，如生命权、身体权、健康权、财产权等。因此，在事前解释与事后解释中，自动化决策方式与个人权益是两者的共同要件，但两者对“重大影响”的判断并不相同。

（一）敏感个人信息处理中对重大影响的推定

事前解释中的“重大影响”为“可能的重大影响”。对于“重大影响”这一要件，《个人信息保护法》第 24 条第 3 款与 GDPR 第 22 条的规范表述并不相同。GDPR 第 22 条将数据主体不受自动化决策限制的要件列为“对数据主体产生法律效力或对其造成类似的重大影响”，从文义结构上看，产生法律效力应属于“重大影响”的一种具体表现。我国《个人信息保护法》第 24 条第 3 款仅要求“重大影响”，但从规范目的而言，“重大影响”应包含产生法律效力这一种表现形式。

遍阅《民法典》，并无“重大影响”这样的表达，与此类似的仅有《民法典》第 496 条中的“重大利害关系”。“重大利害关系”的认定可参考《消费者权益保护法》第 26 条第 1 款，如商品或者服务的数量和质量、价款或者费用、履行期限和方式、安全注意事项和风险提示、民事责任等内容属于与消费者有重大利害关系的范畴。通常认为，《民法典》第 470 条规定的合同一般条款均属于与当事人有重大利害关系的条款。〔46〕具体到个人信息保护领域，若个人信息处理者基于同意而实施个人信息处理行为，“重大利害关系”不仅表现为同意范围内的事项，而且包括可能对个人信息主体的民事权利产生重大影响的内容。若个人信息处理者基于订立合同必需而实施信息处理行为，“重大利害关系”则主要表现为合同这一基础关系所构建的权利义务关系。抽象而言，“重大利害关系”涵括任何对个人信息主体民事权益产生影响的内容。这样的理解也进一步回应了“重大影响”应该包含“产生法律效力”的解释。

《个人信息保护法》第 55 条及第 56 条对于个人信息保护影响评估作出了规范，要求个人信

〔45〕 参见前引〔4〕，解正山文。

〔46〕 参见最高人民法院民法典贯彻实施工作领导小组主编：《中华人民共和国民法典合同编理解与适用》[一]，人民法院出版社 2020 年版，第 246 页。

息处理者在事前应当进行个人信息保护影响评估，评估的内容包含“对个人权益的影响及安全风险”。具体而言，《信息安全技术个人信息安全影响评估指南》（GB/T 39335—2020）第5.5.1对个人权益维度进行了细化。对个人权益的影响可分为以下四类：第一，限制个人自主决定权，例如无法选择拒绝个性化广告的推送，被蓄意推送影响个人价值观判断的资讯等。第二，引发差别性待遇，例如因疾病、婚史、学籍等信息泄露造成的针对个人权利的歧视。第三，使个人名誉受损或遭受精神压力，例如被他人冒用身份、监视追踪等。第四，人身财产受损，例如引发人身伤害、遭受诈骗、勒索等。这些可能对个人权益产生重大影响的内容与《个人信息保护法》第28条中的“人格尊严受到侵害、人身财产安全受到危害”高度吻合。因此，在事前解释中，通过个人信息的敏感度即可推定对个人权益的重大影响。

从《个人信息保护法》第28条至第30条的规定可以明显看出法律对敏感个人信息的特殊保护。敏感个人信息是一旦泄露或者非法使用则容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息（《个人信息保护法》第28条），在个人信息处理过程中容易对个人权益产生重大影响。基于此，个人信息处理者处理敏感个人信息的，应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响，但在一般个人信息的处理中，并未要求个人信息处理者事前告知自动化决策对个人权益的影响。损害尚未实际发生时，对个人信息主体的保护力度应低于损害实际发生的时候。因此，需通过区分个人信息的类型对事前解释作出限制，事前解释的对象应限于对敏感个人信息的处理行为。非敏感的个人信息一般不会引起对个人权益的重大影响，且在事前难以证明。若将非敏感的个人信息的处理纳入事前解释的范畴，会对个人信息处理者课加过重的解释负担。

在符合上述要件后，事前解释的具体内容不仅包括《个人信息保护法》第17条的内容，亦应包括向个人信息主体披露自动化决策适用的逻辑和可能的一般性后果。〔47〕但个人信息处理者仅需作抽象解释，并不具体到与相对人有关的自动化决策结果。〔48〕欧洲法院对算法解释的内容采取了较为谨慎的态度，其指出责任主体仅需对一般性的信息以可理解的方式作出解释。〔49〕事前解释的目的在于帮助个人信息主体了解预期或未来的自动化决策，以便在知情的基础上决定是否允许自己的个人信息被处理、评估自动化处理的合理性或者行使更正权、反对权等请求权。〔50〕通过对系统功能等抽象内容的解释，已经足够达到相应的防御效果。〔51〕

（二）个人同意与解释义务的免除

若个人信息主体事前同意免除个人信息处理者的算法解释义务，会对该义务产生何种影响？免除算法解释义务的事前同意与《个人信息保护法》第13条第1款第1项中规定的“取得个人

〔47〕 See GDPR Article 13（2）（f）、Article14（2）（g）.

〔48〕 参见前引〔10〕，姜野、李拥军文。

〔49〕 See YS v Minister voor Immigratie，Integratie en Asiel（C－141/12）and Minister voor Immigratie，Integratie en Asiel v M，S（C－372/12），ECJ judgment of 17/07/2014 para. 50 et seq.

〔50〕 See Sandra Wachter et al.，Counterfactual Explanations without Opening the Black Box：Automated Decisions and the GPDR，31 *Harvard Journal of Law & Technology* 841，865－867（2018）.

〔51〕 See Antoni Roig，Safeguards for the Right not to be Subject to a Decision Based Solely on Automated Processing（Article 22 GDPR），8 *European Journal of Law and Technology* 1，3（2017）.

的同意”并非等同的概念。前者同意的内容为免除将来的算法解释义务，是对责任的免除；而后者仅同意个人信息处理者对个人信息的处理行为，并非对责任的免除。对于何种情形下能够免除个人信息处理者的解释义务，目前并无细致的研究，仅有学者就免除告知义务主张应当以个人信息是否直接向信息主体收集作为区分标准。〔52〕但这与解释义务的免除并不相同，事前告知义务的内容仅可被事前算法解释所涵括，忽视了事后解释的类型。无论是告知义务的免除还是解释义务的免除，均属于对个人信息主体权益的处分，在适用情形上可参考类似的规范。

《个人信息保护法》第 24 条第 3 款未对算法解释请求权的行使设置例外。GDPR 第 22 条第 2 款设置了 3 项例外情形，第一项是“该决定为订立、履行个人作为一方当事人的合同所必需”，合同作为双方当事人分配风险的工具，若该自动化决策系双方经过自由磋商而订入合同且合同不存在无效情形，则可视为对抗解释义务的事由。第二项是“该决定是由欧盟或其成员国的法律授权作出的，且该欧盟或其成员国的法律不仅约束控制者，并且明确了保护数据主体权利、自由和合法利益的适当措施由联盟或成员国的法律规定”，此种例外情形是指存在明确的法律授权保障该自动化决策的实施，置于我国法律规范的语境下类似于“法律、行政法规规定的其他情形”。如果该自动化决策的决定系为履行法定职责或者法定义务所必需，除非该法定职责或者义务包含无需针对自动化决策作出解释的内容，一般不允许其直接对抗解释义务。但我国《个人信息保护法》第 13 条第 1 款第 4、5 项的内容系基于保护公共利益的目的而设置，公共利益的保护可通过限制个人信息处理者的信息处理行为而实现，限制个人信息处理者的算法解释义务并不能达到此种规范目的，因此无需将其作为免除解释义务的场合处理。第三项是“该决定基于个人信息主体的明确同意”，此处的“明确同意”与个人信息保护中的“告知—同意”规则并不相同。“告知—同意”规则仅针对《个人信息保护法》第 17 条的告知事项，并不包含解释义务中所指向的算法规则与具体决策结果之间的关联。“明确同意”的实质为个人信息主体明知自动化所作出的决定可能会或者已经对个人权益产生重大影响仍愿意接受该种结果的发生。

关键在于，个人信息主体通过事前同意免除解释义务是否有效。个人同意系属于私主体对自己个人信息权益的处分，〔53〕对于个人信息保护中个人信息主体的“同意”的性质，学界存在诸多争议，大致为“法律行为许可说”〔54〕“信托授权行为说”〔55〕“持续性代理行为说”〔56〕等。从民法的角度而言，“同意”的性质应当区分合同与侵权不同的场合而定。在合同领域，同意可能成为合同中给付内容的一部分。在侵权领域，同意或可作为免责事由（受害人同意）免除个人信息处理主体的责任（发生在事后解释的情形下）。〔57〕

通过事前同意免除解释义务的方式分为三种，其一为个人信息处理者提供格式条款排除其解

〔52〕 参见程啸：《论个人信息处理者的告知义务》，载《上海政法学院学报（法治论丛）》2021 年第 5 期。

〔53〕 参见万方：《个人信息处理中的“同意”与“同意撤回”》，载《中国法学》2021 年第 1 期。

〔54〕 参见刘召成：《人格商业化利用权的教义学构造》，载《清华法学》2014 年第 3 期。

〔55〕 参见丁晓东：《个人信息权利的反思与重塑——论个人信息保护的适用、前提与法益基础》，载《中外法学》2020 年第 2 期。

〔56〕 See Jennifer Barrigar et al., Let's Not Get Psyched Out of Privacy: Reflections on Withdrawing Consent to the Collection, Use and Disclosure of Personal Information, 44 *Canadian Business Law Journal* 54, 60 (2006).

〔57〕 参见前引〔53〕，万方文。

释义务，其二为个人信息主体与个人信息处理者磋商达成免除解释义务的约定，其三为个人信息主体单方免除个人信息处理者的解释义务。第一种方式较为常见，典型情形为网络平台设置格式条款，如“用户若同意上述内容，则本平台无需对自动化决策所作出的决定承担解释责任”。个人信息主体仅有是否接受免除解释义务的选择空间，并无磋商余地。但格式化条款可能因排除个人信息主体的主要权利而无效。根据网络平台对自身解释义务减轻或免除的不同程度，分别可能符合《民法典》第497条第2项或第3项，即个人信息处理者通过格式条款不合理地免除或者减轻其责任、加重对方责任、限制对方主要权利和信息处理者直接排除对方主要权利的情形。个人信息主体对个人信息处理者所享有的算法解释请求权是否属于“主要权利”？前文虽否定独立的算法解释权，但算法解释在合同领域中可辅助主权利的实现，对该义务的违反会造成利用个人信息提供服务这一主给付义务的不适当履行。因此，对算法解释的保护应纳入该条所规定的“主要权利”的范畴。第二种方式是个人信息处理者与个人信息主体通过磋商达成免除解释义务的约定。解释义务产生的前提是对个人权益的重大影响，若此种影响已经足以造成对方人身损害或者属于因故意或重大过失造成对方财产损失的，则因违反《民法典》第506条而归于无效。第三种方式是个人信息主体直接单方免除其解释义务，其无效的情形与第二种方式相同。

事前同意免除解释义务，是否需要严格限定于“明确同意”的情形？若个人信息主体默示同意，是否发挥相应的免除效果？在意思表示的概念中，应区分两个方面：作为行动的意思表示以及作为客观逻辑的意义构造的意思表示。只有某一举动本身是被意愿的，才存在一项民法意义上的具有法律重要性的“行动”。〔58〕设置为明确同意的意义在于，自动化决策可能对个人权益产生重大影响，若被免于解释，个人信息主体的同意实际上是对相关合同责任或侵权责任的豁免，意思表示必须清楚且确定，以避免引起权利义务关系的争议。对于默示的意思表示，由于在个人信息处理中存在个人信息主体知情权与个人信息处理者告知义务的断层，同意的意思表示本就存在不自由的空间，〔59〕若允许默示同意，则难以避免个人信息主体作出含有效力瑕疵的意思表示。

因此，个人信息处理者的解释义务不可轻易被事前免除，若自动化决策可能对个人信息主体的权益产生重大影响，个人信息处理者需对自动化决策的相关内容作出清晰、通俗的解释。《个人信息保护法》第24条第3款并未规定违反该事前解释义务的民事责任，需具体分析：若双方将解释义务订入合同约定，则依照是否违反合同义务界定民事责任；在无合同约定的场合，个人信息主体可拒绝个人信息处理者仅依据自动化决策作出决定。而事后所产生的解释义务以及损害赔偿义务可被免除，原因在于当事人可对自己已经产生的算法解释请求权及损害赔偿请求权予以处分，与事前免除的效果存在本质区别。

三、事后解释在救济体系中的功能与损害赔偿

事后解释中的关键要件是“已经对个人权益产生实际的重大影响”，且无论是一般个人信息

〔58〕 参见〔德〕卡尔·拉伦茨：《法律行为解释之方法——兼论意思表示理论》，范雪飞、吴训祥译，法律出版社2018年版，第36－37页。

〔59〕 参见前引〔53〕，万方文；武腾：《最小必要原则在平台处理个人信息实践中的适用》，载《法学研究》2021年第6期。

还是敏感个人信息，只要符合该要件即可要求事后解释。原因在于，重大影响或者损害已经实际产生，既不会对个人信息处理者造成过重的解释负担，亦有正当理由反驳以商业秘密为抗辩。至于何种结果构成“重大影响”，需在合同或侵权等不同场域分别判断。在重大影响已经实际产生的情况下，事后解释并不能发挥完全的救济效果，需辅之损害赔偿责任。

（一）事后解释中的重大影响

事后解释中重大影响的典型一般为不当处理个人信息，导致个人在工作机会、金融安排等方面遭受负面影响。〔60〕一方面包括自动化决策对个人信息主体的法律地位或合同权利等产生影响，如合同撤销、社会福利丧失、被拒绝给予公民身份等；另一方面也包括个人的法律权利或义务未因自动化决策而改变，但是该决策对个人的境遇、行为或选择产生显著影响，或导致其因歧视被排除在某种机会之外（如金融服务、就业或者教育机会丧失）。〔61〕但根据《个人信息保护法》第 24 条第 3 款的文义，“重大影响”并未限定于不利影响的层面，即便是产生有利的重大影响，个人信息主体仍有选择是否接受的自由。

鉴于上述讨论，何种行为可被评价为“对个人权益已经产生重大影响”乃问题的核心。个人权益的认定与影响是否重大存在直接的关联，该问题可转化为如何认定构成重大影响的个人权益。在合同关系中，个人信息处理对个人权益产生重大影响的典型表现为个人信息处理的格式条款，网络平台多基于此声明有权对个人信息进行收集、存储、使用等。因此，对《民法典》第 497 条中“主要权利”的判断可资借鉴，但何为“主要权利”，需要根据合同性质本身确定，不仅仅关注双方当事人签订合同的内容，而应就合同本身的性质来考察。〔62〕“主要权利”不可简单地解释为法律规定的权利，或由法院基于公平原则进行自由裁量所认定的权利。〔63〕因此，“对个人权益已经产生重大影响”在合同领域表现为违反主给付义务以及违反其他给付义务导致个人权益遭受损害，在侵权领域表现为对个人信息主体主要权利造成损害。

由于此时影响已经实际产生，对于影响程度的判断相较于事前解释中对重大影响的推定更为容易且准确。依据《信息安全技术个人信息安全影响评估指南》（GB/T 39335—2020）中所提供的个人权益影响程度判定准则，可以个人信息主体所遭受的困扰程度、付出的成本、生理疾病、财产权益损害、信用名誉损害等作为标准判断影响的严重程度。若该自动化决策行为使得个人信息主体遭受诈骗、信用评分和名誉受损、失去工作机会、产生生理疾病等，则可被评价为对个人权益产生了重大影响。当然，这些情况在限制个人自主决定权、引发差别性待遇、人身财产受损等不同场景中存在不同的表现，需具体判断。若只是对个人信息主体造成了精神上的厌烦与恼怒情绪，则仅被评价为低程度的影响，不符合要求事后解释的要件。

在事后解释中，算法控制者应当向个人信息主体披露的信息不限于算法系统功能的一般性事前解释，而应对具体的算法决策结果予以说明，如基础性数据、算法规则、决策结果三者之间的

〔60〕 See Christopher Kuner et al., *The EU General Data Protection Regulation (GDPR) A Commentary*, Oxford University Press, 2020, p. 523, 666.

〔61〕 See A29WP: A29 WP, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, 17/EN. WP 251rev. 01 (Feb. 6, 2018).

〔62〕 参见前引〔46〕，最高人民法院民法典贯彻实施工作领导小组主编书，第 253 页。

〔63〕 参见杨显滨：《网络平台个人信息处理格式条款的效力认定》，载《政治与法律》2021 年第 4 期。

关联性。〔64〕可能面临的困境在于，打开“算法黑箱”不可避免地涉及对定义代码和算法规则的专业解释，高维机器学习人类解释风格在技术素养方面的差异造成了算法透明度的一大障碍。〔65〕此时需要由该自动化决策所涉及的具体领域的专业人士作出阐释，如医疗服务者可以解释手术与辐射治疗的差异，对每个技术细节进行解释，〔66〕以辅助判断决策作出的正当性。

（二）损害赔偿认定中的算法解释

事后履行解释义务所发挥的效果弱于事前解释的防御效果，需要辅之以拒绝、删除，以及合同和侵权领域的损害赔偿责任。《个人信息保护法》第 24 条第 3 款赋予了个人信息主体对仅通过自动化决策作出决定予以拒绝的请求权，主张拒绝的要件应为该决定对个人权益产生了重大影响。因此，个人信息主体有权要求个人信息处理者予以解释说明，在个人信息处理者违反解释义务时，个人信息主体可主张拒绝仅受该自动化决策结果约束，亦可根据《个人信息保护法》第 47 条第 1 款第 4 项的规定主张删除。但“拒绝＋删除”的处理模式仅能面向将来产生保护效力，并不能有效救济已经遭受重大影响的个人权益。

存在重大影响但未造成实际损害的情形下，个人信息主体仅可主张算法解释，存在重大影响且损害已经实际发生的情形则需在主张算法解释后，在个人信息处理者未对该行为作出合理解释的情况下才能主张损害赔偿。是否能够辅之以合同或者侵权责任意义上的损害赔偿请求权，关键在于判断重大影响的结果是否能够被评价为法律意义上的损害。〔67〕依《个人信息保护法》第 24 条第 1 款的规定，个人信息处理者不得对个人在交易价格等交易条件上实行不合理的差别待遇。此种差别待遇构成价格歧视，在合同关系领域可能构成欺诈或者显失公平，其损害的是个人信息主体的财产权益。但该条第 2 款所提及的信息推送、商业营销等针对个人特征的选项若未采取滥用市场支配地位、故意悖俗地使用算法造成排除、限制竞争或者损害消费者福利等行为时，不可被直接认定为对个人信息主体构成了损害。因此，是否能够主张合同或者侵权责任上的损害赔偿请求权，需根据《民法典》第 584 条或第 1182 条至 1185 条的规定具体判断。

“未合理履行算法解释义务”这一行为在合同法上与侵权法上的评价存在区别。在传统民法中，侵权行为与违约行为均为债的发生原因，前者产生法定之债，后者产生意定之债。〔68〕从用户角度出发，数据活动关系人可通过用户协议（个人信息授权合同）的方式建立数据收集、利用的债之关系。〔69〕如在定制信息推送、智能投顾、搜索引擎等典型场合，算法提供者的主给付义务在于为个人提供上述核心服务功能，而算法解释旨在避免算法决策对当事人的个人权益产生重大影响，可被合同关系中的保护义务所涵盖。〔70〕算法解释义务在合同领域表现为对合同履行行

〔64〕 See GDPR Article 15 (1) (h).

〔65〕 See Bryce Goodman, Seth Flaxman, European Union Regulations on Algorithmic Decision-Making and a Right to Explanation, 38 *AI Magazine* 50, 55 (2017).

〔66〕 See Tae Wan Kim, Bryan R. Routledge, Informational Privacy, A Right to Explanation, and Interpretable AI, in 2018 *IEEE Symposium on Privacy-Aware Computing* (*PAC*), IEEE, 2018, pp. 64－74.

〔67〕 参见王泽鉴：《损害赔偿》，北京大学出版社 2017 年版，第 62 页。

〔68〕 参见程啸：《侵权责任法》（第 3 版），法律出版社 2021 年版，第 79 页。

〔69〕 参见龙卫球：《数据新型财产权构建及其体系研究》，载《政法论坛》2017 年第 4 期。

〔70〕 对于“给付义务—保护义务”这一分类，参见张家勇：《合同法与侵权法中间领域调整模式研究——以制度互动的实证分析为中心》，北京大学出版社 2016 年版，第 199－200 页。

为符合双方缔约目的的解释义务。若个人信息处理者未能解释对个人权益产生重大影响的自动化决策条款或者自动化决策结果，则分别导致该条款未被订入合同或个人信息处理者承担相应违约责任的后果。有观点认为算法服务提供者的算法解释属于合同法上的从给付义务与附随义务，〔71〕实际上也是承认算法解释作为合同义务保护当事人合法权益的本质。

因此，当个人信息处理者与个人信息主体处于合同关系中时，“未合理履行算法解释义务”应被评价为债务不履行。当事人将“自动化决策决定对个人权益产生重大影响则可要求个人信息处理者作出解释”订入合同条款并不能将解释义务的性质划定为合同的主给付义务。原因在于，合同的主给付义务内容为个人信息主体按要求提供相关个人信息并获得服务，个人信息处理者依据个人信息主体提供的个人信息作出自动化决策并提供服务。但算法解释义务与主给付义务内容密切相关，其性质为合同保护义务，对该义务的违反亦构成主给付义务的不适当履行，个人信息主体可据此主张违约损害赔偿。

在个人信息处理者与个人信息主体并未进入合同这一特别结合关系时，“未合理履行算法解释义务”不可被评价为侵权法上的“侵权行为”，而应被评价为“过错”。对于侵权请求权中“过错”要件的举证需通过算法解释辅助说明，如个人信息处理者无法解释或者拒绝解释则应推定个人信息处理者存在过错。侵权行为所违反的是法定义务、绝对义务，〔72〕侵害的对象一般为绝对权。算法解释义务作为人格权所衍生的非独立性请求权，并不具有绝对义务的性质。违反算法解释义务本身并非侵权行为，对个人权益造成重大不利影响的个人信息处理才属于个人信息保护中的侵权行为。需要注意的是，《个人信息保护法》第 24 条第 3 款所规定的“个人权益”并不仅限于个人信息权益，亦包括其他权益。典型如算法处理个人信息过程中对个体的信用评级造成重大不利影响，侵害了信用权（《民法典》第 1029 条）。因此，应将“未合理履行算法解释义务”评价为过错，但需要厘清的是归责原则为一般的过错责任原则还是过错推定责任，这与举证责任的分配以及不利后果的承担密切相关。

本文从民法体系出发，将个人信息处理关系限定在采用自动化决策的非公务机关与个人信息主体之间。在此种关系类型中，双方当事人在举证责任和诉讼能力上的差异主要是由“自动化决策技术”造成的，若采用一般过错归责原则，鉴于自动化决策技术中蕴藏的算法复杂性，可能会对个人信息主体课加过重的举证负担，〔73〕因此应采过错推定原则。〔74〕《个人信息保护法》第 69 条第 1 款规定了个人信息权益致害以过错推定原则归责，〔75〕处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任，目的在于维持权益保护与产业发展的平衡。〔76〕虽然个人信息侵权中的损害具有无形性、潜伏性、未知性等

〔71〕 参见鲁春雅：《自动化决策的算法解释权——以合同义务为视角》，载《中国社会科学报》2020 年 12 月 23 日，第 4 版。

〔72〕 绝对义务是指个人具有与不定数目的人或其他所有人有关的义务。参见〔奥〕凯尔森：《法与国家的一般理论》，沈宗灵译，商务印书馆 2013 年版，第 140 页。

〔73〕 有法院认为：“从收集证据的资金、技术等成本上看，作为普通人的庞理鹏根本不具备对东航、趣拿公司内部数据信息管理是否存在漏洞等情况进行举证证明的能力。”北京市第一中级人民法院（2017）京 01 民终 509 号民事判决书。

〔74〕 参见叶名怡：《个人信息的侵权法保护》，载《法学研究》2018 年第 4 期。

〔75〕 参见前引〔32〕，程啸书，第 506 页。

〔76〕 参见谢鸿飞：《个人信息泄露侵权责任构成中的“损害”——兼论风险社会中损害的观念化》，载《国家检察官学院学报》2021 年第 5 期。

诸多与传统侵权场域不同的特殊性，〔77〕但在自动化决策处理个人信息的场合，关键在于证明算法规则具有合理性且未对个人权益产生重大不利影响，以算法解释作为评价个人信息处理者过错的衡量标准。“不能证明自己没有过错的”不仅包括个人信息处理者履行解释义务后无法证明决策结果合理性的情形，亦包括个人信息处理者拒绝履行算法解释义务的情形，拒绝解释视为放弃举证而直接负担不利后果。

值得讨论的是，是否需对敏感个人信息与非敏感个人信息的归责原则作区分处理。有观点认为处理敏感个人信息应适用无过错责任，处理非敏感个人信息适用过错推定责任，原因在于敏感个人信息的处理行为开启了危险源，处理者对处理行为具有控制力，应承担更严格的责任。〔78〕在本文的语境下，个人信息处理为私主体之间的关系，并不包括公务机关，双方对于危险控制的差异在于算法技术的控制权，采用过错推定责任已经对个人信息处理者设定了自律机制，以增强其处理过程中的责任心。〔79〕对敏感个人信息与非敏感个人信息的区别保护可通过调整算法解释义务即举证责任的方式实现。在敏感个人信息处理的场合，个人信息处理者的举证责任更重，原因在于敏感个人信息相较于一般个人信息更容易在处理过程中受到侵害，对算法规则设计的合理性要求更高。若在敏感个人信息处理中适用无过错原则，相当于将处理敏感个人信息的行为直接视为危险责任，既是对算法解释义务作为过错评价功能的忽视，亦不利于解决个人信息流通与个人信息保护之间的利益冲突。综上，若个人信息处理者拒绝履行解释义务或者履行解释义务后并不能证明其无过错，则损害赔偿的不利后果由其承担。至于损害赔偿的范围，依《个人信息保护法》第 69 条第 2 款具体确定，赔偿范围包括财产损害与精神损害。

四、结　论

现代性正以前所未有的方式，把我们抛离了所有类型的社会秩序的轨道，从而形成了其生活形态。这一点在技术方面表现得尤为显著，并逐渐渗透至其他领域，引发信任与风险的紧张关系。〔80〕个人信息应作为人格中纯粹的一部分，不可简单地沦为促进他人增益或者实现社会目的的手段。从民法体系的视角观察，算法解释背后所保护的个人信息权益应为人格权益，算法解释请求权的本质是为人格权服务的非独立请求权。在合同关系领域，算法解释可纳入合同保护义务的范畴以助于主给付义务的履行，个人信息处理者可能因违反解释义务承担相应的违约责任。在侵权领域，算法解释则作为过错评价的要素发挥作用，即自动化决策对个人权益产生重大影响可否被评价为侵权行为，需以个人信息处理者履行算法解释义务的结果作为辅助判断的标准。

为缓解个人信息权益保护与个人信息利用之间的紧张关系，算法解释应区分为事前解释与事后解释两种类型。事前解释仅适用于敏感个人信息的自动化决策场合，因为在事前无法对一般个人信息是否产生重大影响作出准确的判断，而敏感个人信息的处理基于其个人信息类型的敏感度

〔77〕 参见田野：《风险作为损害：大数据时代侵权“损害”概念的革新》，载《政治与法律》2021 年第 10 期。
〔78〕 参见程啸：《侵害个人信息权益的侵权责任》，载《中国法律评论》2021 年第 5 期。
〔79〕 参见申卫星：《论个人信息保护与利用的平衡》，载《中国法律评论》2021 年第 5 期。
〔80〕 参见〔英〕安东尼·吉登斯：《现代性的后果》，田禾译，译林出版社 2011 年版，第 4－8 页。

即可推定出可能会对个人权益产生重大影响。重大影响实际产生后的事后解释则无需区分个人信息的敏感程度。此时若产生了损害，单纯的事后解释与“拒绝＋删除”模式并不能发挥全面的救济功能，需辅助以合同法或者侵权责任上的损害赔偿责任。是否承担合同损害赔偿责任取决于是否违反合同义务。在侵权损害赔偿中，若个人信息处理者无法解释或者拒绝解释则推定其存在过错并承担不利后果。

Abstract: From a civil law perspective, personal information should be protected as a legal interest. The algorithmic interpretation of automated decision-making is in fact a non-independent claim derived from personality rights and does not require the creation of a separate right of algorithmic interpretation. In the field of contract, algorithmic interpretation can be included in the scope of the duty of protection, while in the field of tort, it has the function of fault evaluation, and when the personal information processor is unable to explain or refuses to explain, it can be presumed to be at fault. In order to protect the commercial secrets of personal information processors and reduce their burden of interpretation, the algorithmic interpretation stipulated in Article 24 (3) of the Personal Information Protection Law shall be distinguished into two types: ex ante interpretation and ex post interpretation, which differ in terms of the construction of the elements and the degree of interpretation. The ex ante interpretation shall be limited to the handling of sensitive personal information that “may have a significant impact”, while the ex post interpretation shall occur in the case of automated decisions that “already have a significant impact on the rights and interests of individuals”. The duty of ex ante interpretation should be lower than that of the ex post interpretation, which corresponds to an abstract interpretation of the system's function and a detailed interpretation of a specific decision respectively. In the event of actual damage arising from the material impact, the subject of personal data may claim liability for damages in breach of contract or tort. Intentional exemptions from the obligation to interpret ex ante shall be void if they violate Article 497 or Article 506 of the Civil Code, but the obligation to interpret ex post and the right to claim damages arising therefrom may be exempted.

Key Words: algorithmic interpretation, interest in personal information, automated decision-making, significant impact

（责任编辑：殷秋实　赵建蕊）

财经法学 No. 4，2022
pp. 115 - 131

破产程序中数据权益之保护
——以信义义务为视角

程　威*

内容提要：破产程序中数据权益保护问题渐受重视，而现行物权、合同、知识产权等适用规则对此面临保护不足、调整失当的困境。比较法所确立的个人控制论立场，从数据主体锁定数据使用流向的视角出发，对数据权益的商品化约束过甚，无法调息数据人格权益与财产权益的内在冲突，并与破产程序中债务人财产价值最大化的理念相悖离。应重视数据主体与数据控制者之间信赖关系的建构，根据信义义务构成要件理论与破产法的团队生产理论，在破产程序中为数据控制者施加保密、安全、透明与忠实的受托人义务，并根据场景化的路径在数据平台企业与经营管理层之间妥善分配责任，通过强制性的法定责任约束，为数据控制者在破产程序中提供行为指引，以强化对数据主体权益在破产程序中的保护。

关键词：数据权益　数据控制者　信义义务　团队生产理论　场景化规制

自 2012 年全国人大常委会通过《关于加强网络信息保护的决定》以来，对个人数据保护的立法活动不断加快脚步，采取强有力的策略保护个人数据已经成为共识。相关的中文研究成果迅速积累，但有关文献所侧重的场景，主要围绕数据平台企业（数据控制者）在企业正常、健康运转过程中与数据主体之间在法律利益上的配置。当企业因不能清偿到期债务或资产不足以清偿全部债务而面临破产时，如何处理相关数据，对此研究不足。特别是数据平台企业以数据资源为其资产升值的引擎，对数据权益的争夺将使得数据主体与数据控制者陷入紧张关系——平台企业是否以及如何处理数据资产及其权益？近年来，如小鸣单车等储备海量数据资源的企业陷入破产，

*　程威，华东政法大学经济法学院助理研究员。

本文为国家社科基金项目“关联企业实质合并破产判断规则的制度化进路研究”（17CFX030）、安徽大学经济法制研究中心招标项目（pcs2021yjs-6）的阶段性成果。

其核心问题即在于此。〔1〕

破产程序中，数据权益处理需受重视。事实上，在财务稳健时期，企业数据资源向第三方出售、分享等处理行为已然有之，我国《个人信息保护法》将处理界定为收集、存储、使用、加工、传输、提供、公开等活动，尽管有学者认为这一界定因未对处理行为进行抽象提取且采开放列举，造成概念内涵与外延不甚清晰，〔2〕然而可以明确的是，其覆盖破产程序中使数据在主体之间单向与双向传输等行为。个人数据在传输过程中涉及个人对数据利益的期待，其内容不仅包括敏感信息所附载的隐私利益期待，还有数据主体对数据信息所享有的自决权的期待，即非敏感信息的自我保护。〔3〕取得数据主体同意是处理行为之前提与神圣法则。然而这一规则对数据权益的商品化约束过甚，不利于破产程序中债务人财产最大化目标的实现。对于这些问题，我国立法上并未给予明复。在《个人信息保护法》推行贯彻，以及《企业破产法》修订工作展开的现实背景下，有必要对此一问题给予立法论上的考量。在中文语境下，个人数据与个人信息可能存在内容与形式的差异，〔4〕但法律意义上二者内涵相同，具有内在一致性，为便于论述，本文主要使用“个人数据”的表达。

一、破产程序中数据权益保护的法律挑战

我国 2020 年《信息安全技术/个人信息安全规范》（以下简称“2020 规范”）9.3 条规定当个人信息控制者发生收购、兼并、重组、破产等变更时，应当满足以下要求：个人信息控制者应当向个人信息主体告知有关情况；变更后的控制者应继续履行原信息责任与义务，如变更个人信息使用目的，应重新取得信息主体明示同意；如破产且无承接方的，对数据做删除处理。这为解决破产中数据处理提供了原则性指导，但并不能真正解决破产程序中数据权益的处理问题，原因在于：首先，该规范本身的法律效力层级属于部门规章，缺乏对于数据权益性质的定义性规范，并不能产生确权与保护的效果，一定程度上是解决个案问题的权宜之计，难以构造稳定的权利保护预期；其次，如果将之视为在破产状态下的特定处理方式，从而绕开基本权益性质的探讨，尽管具有解释上的合理性，却缺乏法理上的规定性。破产程序作为一种集体清偿机制，其所赖以存在的原理基础是对原权利的默示认同，根据债权人谈判理论，尊重非破产法规范是破产制度的前提，只有当事人保有破产前之权利位序、强度，才得以在破产程序推进过程中展开有效的谈判，从而达致债务人财产价值最大化。〔5〕除非有特别的理由，否则不应支持对财产权益的调整。〔6〕

相应地，从现有的实体性法律规范出发界定数据权益之于破产程序的意义，属于必要的检验

〔1〕 参见广州市中级人民法院（2018）粤 01 破 12—1 号民事裁定书。

〔2〕 参见高富平：《个人信息处理——我国个人信息保护法的规范对象》，载《法商研究》2021 年第 2 期。

〔3〕 参见叶名怡：《个人信息的侵权法保护》，载《法学研究》2018 年第 4 期。

〔4〕 关于数据、隐私、信息之间法理关系的细化分析，参见彭诚信：《数据利用的根本矛盾何以消除——基于隐私、信息与数据的法理厘清》，载《探索与争鸣》2020 年第 2 期。

〔5〕 See Douglas G. Baird, Thomas H. Jackson, Corporate Reorganization and the Treatment of Diverse Ownership Interests: A Comment on Adequate Protection of Secured Creditors in Bankruptcy, 51 *University of Chicago Law Review* 97, 103 (1984).

〔6〕 不轻易改变规则的主要原因是防止打破原有的实体法规范预期从而扭曲当事人的激励。参见前引〔5〕，Baird、Jackson 文，第 103 页。

步骤，也是破产法律制度的基本要求。实际上，如后文的检验结果所示，传统物理世界的规范表达并不能够回应数字化时代企业破产时的权利诉求。

（一）物权法的适用

适用物权机制理解数据权益必然着眼于权利主体。我国学者在这一论证视角下将其分为两种类型，即数据私有与数据公有，〔7〕在此基础上可进一步细化为四种子类型：数据个人所有、数据平台所有、数据个人与平台共有、数据公众所有。〔8〕但是将这一分类规范应用到破产法的世界，均会构成无法逾越的解释困境和不利后果。

如果将数据视为个人所有，破产时数据主体可以行使取回权以获取属于己身的权益，而此时别除权的对象是个人在使用平台企业提供服务过程中自行提交的数据信息，还是应当包括平台企业对该信息进行算法挖掘形成的加工数据？对于前者，数据主体并不需要通过行使权利的方式获取，因为该数据内容之于数据主体是不言自明的；而对于后者，设若将加工数据复制传输给所有被利用信息的数据主体，且不说该类信息之于数据主体而言不具实益，传输数据的成本对于陷入破产境地的企业而言更不可欲。

如果将数据视为平台所有，从根本上否定了数据主体提交数据行为时所含有的隐私期待，破产事件触发后将无法回应数据主体的利益保护。当认为数据归个人与平台共有时，个人与平台在破产程序中的权力边界划分仍然无法拆解。尽管我国司法机关在这一观点上走得很远，并发展出“用户授权＋平台授权＋用户授权”的“三重授权”模式，强调数据主体可以通过两重授权遏制平台不合理的行为，但这一裁判理念是以个案分析为基础，〔9〕当进入破产程序时，强行要求平台企业取得所有用户主体的同意并不现实。〔10〕将数据视为公共所有，建立在互联网公共属性认知的基础之上，〔11〕但其完全忽视私益保护，因为当企业破产时，该集体利益上的数据主体会产生集体行动的困境，各个主体理性漠视集体权益的维护，最终产生类似于公地悲剧式的权益毁损结果。

（二）合同法的适用

适用合同法的立足点是将数据主体与数据控制者之间的关系设定为数据服务合同。在破产程序中，数据服务合同囿于相对性原则的约束，难以回应破产情事所对应的大规模债权清偿的问题，特别是服务合同作为未典型化的无名合同，因其标的之非物质性、劳务行为折算成金钱之不确定性等，造成与传统破产法待履行合同解除权与共益债务规则的冲突。

具言之，数据服务合同非即时性合同，而具有持续履行的特征，在平台企业破产时，可将其纳入待履行合同范畴。对此，《企业破产法》第18条规定管理人享有决定解除或继续履行的选择权，设若管理人选择解除合同（拒绝履行），“合同相对人基于双务合同的原给付非金钱债权便在

〔7〕 参见韩旭至：《数据确权的困境及破解之道》，载《东方法学》2020年第1期。

〔8〕 参见丁晓东：《数据到底属于谁？——从网络爬虫看平台数据权属与数据保护》，载《华东政法大学学报》2019年第5期。

〔9〕 参见北京市海淀区人民法院（2015）海民（知）初字第12602号民事判决书。

〔10〕 参见前引〔8〕，丁晓东文。

〔11〕 See Orin S. Kerr, Norms of Computer Trespass, 116 *Columbia Law Review* 1143, 1163 (2016).

破产程序中按照数额转化为金钱债权，作为普通债权向管理人申报”〔12〕，此时，数据控制者在数据服务合同履行期间对数据服务本身所享受到的利益，是否得与为数据主体提供服务所转化的利益相抵消，不无疑问；若管理人选择继续履行，则数据主体的普通债权便升级为“共益债务”，获得升级效果，〔13〕但问题在于，此时继续履行之数据服务并未给数据主体造成权益损失，破产企业或经由重整或经由收购至其他同类企业而得以延续，此时按照权益损害的救济逻辑而另行为数据主体提供价金之补偿，难谓有正当性。

（三）知识产权法的适用

知识产权法所适用的具体含义是：数据控制者通过对数据（特别是加工数据）享有汇编意义上的版权而反制爬虫等侵权行为；数据控制者以对数据信息享有商业秘密而获得竞争法与知识产权法上的保护；数据控制者对著作权保护之外的数据可根据数据库保护获得救济。然而破产视角下，知识产权法适用路径的根本缺陷，不仅在于保护范围局限于特定内容，更在于其单独偏向于数据控制者而造成法律天平上对数据主体的保护失衡。

首先，著作权虽然具有人格权与财产权双重属性，但该属性必然指向同一主体。〔14〕具言之，在企业破产时，将数据财产权置于数据控制者、将数据人格权置于数据主体的分割思想不合法理，数据主体对数据在人格权意义上的利益期待将会落空。其次，商业秘密的保护实际上是隐私法对商业化保护的延伸，〔15〕尽管注意到其价值意义，但仍然聚焦于数据控制者的利益。更为重要的是，平台企业破产时，商业秘密如严守秘密保护的政策，根本无益于破产企业穷尽一切途径变现增值的追求。最后，数据库保护限定在结构化数据，数据企业破产时是否必然拥有结构化的数据，不具有普遍性，即便针对具有数据库的企业，破产法仍然仅在尊重非破产法规范上保护数据控制者的诉求。

除了以上法律适用路径，对数据的保护尚存在竞争法、消费者保护法、刑法等工具选择。然而此类保护主要在公法层面，具有公共利益导向、社会倾斜性关照的意涵，因其在破产程序中需做例外处理，故不具一般性讨论价值。综上而言，当企业破产时，“不幸的人各有各的不幸”，现有制度无法解答彼时数据权益保护的问题。这也是信息时代对资产属性的界定与工业时代法律制度之间存在冲突的必然结果。企业破产时数据主体的数据隐私期待面临挑战，如何回应这一挑战关系到数据主体能否顺利从数据控制者的经营失败中抽身。比较法上的规则因应或可提供一定的参考。

二、破产程序中数据权益保护的实践因应：个人控制论

（一）美国破产程序中的数据权益

数字经济语境下，数据信息的资产价值甚至超越有形资产，承载姓名、物理地址、电子邮

〔12〕 庄加园、段磊：《待履行合同解除权之反思》，载《清华法学》2019 年第 5 期，第 133 页。

〔13〕 参见前引〔12〕，庄加园、段磊文。

〔14〕 参见王迁：《著作权法》，中国人民大学出版社 2015 年版，第 144 页。

〔15〕 See Daniel J. Solove, *Understanding Privacy*, Harvard University Press, 2008, p. 130.

箱、电话号码、购买历史、个人偏好以及其他类型的数据信息，当破产发生时，平台企业可基于数据分发、算法挖掘等方式实现特定财产化的商业目标，〔16〕损害个人隐私利益现象较易发生，对此理应提供更为切实的保护。

美国法实践中，在企业破产时产生数据隐私保护问题的案件一般是，债务人企业在收集数据主体信息时作出不会转让、共享的承诺，但在破产之前或破产要件触发不久后修改隐私政策以准允企业转让数据信息。〔17〕

1. 制定法立场

在2000年左右，伴随着互联网经济的快速发展，收集个人数据并转化为商业利益的盈利模式已经成熟运转，在企业并购、破产中数据主体更换引发的数据权益保护问题，成为美国破产立法的现实议程。当债务人计划出售个人数据时，为了保护消费者，美国国会修改破产法对“个人可识别数据”的出售施加限制，其前提要件是：（1）债务人企业在收集个人数据时，在隐私政策中明确允诺待破产程序开始时禁止转让个人数据；（2）该隐私政策在破产时仍然生效。〔18〕也就是说，在破产申请时，如果债务人企业的隐私政策禁止出售个人数据，或该隐私政策未能明确披露债务人可以出售个人数据，此时债务人企业为了实现数据出售的目的，应满足以下两个条件之一：（1）出售行为与债务人在破产申请时继续生效的隐私政策相一致；（2）经任命的消费者隐私检察员向法院提供相关评估报告，当发现并无证据显示出售行为违反有效的非破产法规范，法院将批准出售。〔19〕

关于第一项条件，隐私政策的效力基础是告知同意规则，当且仅当数据控制者在收集数据过程中明确征得数据主体的同意，方可形成对数据在特定用途与方式中的使用权。从合同关系视角来看，隐私政策的发出视为要约，而数据主体点击同意视为承诺，两者意思合致构成有拘束力的合同。但为了防止“全有全无式”管理架构和信息茧房造成的心理预期偏差，如果无法判断数据主体是否对隐私政策作出了同意的意思表示（如数据主体点击同意仅仅是为了便于使用软件程序），则出于保护用户个人数据权利的立场，应认定数据主体并未同意隐私政策内容。〔20〕这反映出，当债务人企业出售数据的行为与收集数据主体数据时隐私政策一致时，数据主体对数据隐私权益的预期已经做了肯定性的处分，是对个人权益自行筹划后的理性安排；但凡数据主体在隐私政策签订时并未给定明确同意，当破产开始时，即可要求数据控制者不得出售其数据，或令后者对出售行为承担无权处分的法律责任甚至是可以撤回出售行为。这种对于数据主体权益的保护，根源在于个人控制的强烈立场。

如果说第一项条件直接地反映了个人控制的立场，则第二项条件在一定意义上似乎增加了社会化的考量因素，但循其根本，仍然谨守个人控制的法理基础。具体而言，消费者隐私检察员作

〔16〕 See Walter W. Miller, Jr., Maureen A. ORourke, Bankruptcy Law v. Privacy Rights: Which Holds the Trump Card?, 38 *Houston Law Review* 777, 795 (2001).

〔17〕 See Michael St. Patrick Baxter, The Sale of Personally Identifiable Information in Bankruptcy, 27 *American Bankruptcy Institute Law Review* 1, 2 (2019).

〔18〕 See 11 U.S.C §363 (b) (1).

〔19〕 参见前引〔17〕，Baxter文，第4页。

〔20〕 参见王叶刚：《论网络隐私政策的效力——以个人信息保护为中心》，载《比较法研究》2020年第1期。

为美国联邦托管人（US Trustee）任命的具有公益属性的行政机构事务辅助专员，会提出与可适用的隐私政策相一致的出售方式，以及其他解决隐私问题或减轻隐私损害的手段。就内容上来看，所建议的方式仍然要求拟议出售行为的前提是债务人向消费者通知了转让行为或建议债务人获得受损害消费者的明确同意。〔21〕由是可知，如果债务人破产时，通知后未获得同意或受损害消费者明确表示个人数据从出售的数据包中退出，则数据控制者对此显然须作剔除处理。

制定法的立场虽然考虑到市场效率在债务人破产财产处理中的必要性，但是数据主体的防御性保护仍然是重要的价值判断，增进财产处分便利性不能以牺牲个人控制的期待利益保护为代价。

2. 判例法回应

美国第一起处理破产程序中个人数据保护的案件是著名的 Toysmart 案。Toysmart 是一家在线儿童玩具零售商，其隐私政策中承诺将永远不会与第三方分享所收集到的用户数据。然而在破产时，该公司试图出售包括详细的客户数据在内的信息库等所有资产。该行为引起联邦贸易委员会的重视，后者认为其行为违反了《联邦贸易委员会法案》第 5 条“不公平或欺骗行为”，要求 Toysmart 公司不得违反隐私政策出售客户数据，最终两者达成和解协议，Toysmart 获准在破产程序中出售消费者个人数据，但必须符合以下条件：（1）消费者数据与债务人其他资产一揽子出售而非单独出售；（2）买受人须与债务人处于同一行业，是为合格买受人；（3）买受人同意遵守 Toysmart 此前对消费者个人数据的隐私政策；（4）买受人将消费者个人数据转用其他任何用途之前，须通知受影响消费者并取得后者的明确同意。〔22〕

除 Toysmart 案所确立的示范性规则之外，破产程序中个人数据出售面临的另一项问题是，当债务人企业早先的隐私政策进行了数次调整，特别是为了迎合商业化需求对个人数据出售从保证不分享转为逐步解锁限制，而消费者通常默示同意隐私政策的修改，有观点认为，先前隐私政策下所设定的限制转让的严格要件并不辖制此时的出售行为，此时条件宽松的修改后隐私政策准允在破产程序中出售个人数据，并不违反破产法的规定。但美国联邦贸易委员会对此明确指出，债务人在破产申请日的隐私政策并不是唯一重要的隐私政策，在某些情况下，债务人收集的隐私政策可能受制于在此之前隐私政策中的规定。〔23〕

为了回应这一问题，美国的判例法一般会施加相应的限定条件以保证消费者的数据权益在可控范围内。如 Borders 案中，借助消费者隐私检察员的协助，案涉利益各方在最后达成的拟售决定允许个人数据的出售，而不考虑数据收集的时间点，其前提是：（1）买受人向拟转让其个人识别数据的每个消费者发送一封电子邮件，通知他们要转让的数据信息，并说明他们的个人识别数据将受买受人隐私权政策的约束，并给予 15 天的时间选择退出与否；（2）在 Borders 公司和买受人的官网上发布为期 30 天的转让和退出的通知；（3）债务人在《今日美国》报刊上发布出售与

〔21〕 See In re Old BPS US Holding, Inc., No. 16 - 12373 (Bankr. D. Del. Feb. 1, 2017); In re Borders Group, Inc., 462 B. R. 42, No. 11 - 10614 (Bankr. S. D. N. Y. Dec. 7. 2011).

〔22〕 See FTC Announces Settlement With Bankrupt Website, Toysmart. com, Regarding Alleged Privacy Policy Violations, FTC: PRESS RELEASES (July 21, 2000), available at https://www.ftc.gov/news-events/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom-regarding, last visited on Jan. 19, 2022.

〔23〕 See In re Gateway Learning Corp., FTC Docket No. C - 4120 (F. T. C Sept. 10, 2004).

选择退出的通知。[24] 这种面面俱到的附条件出售限制，均以对数据主体的充分知情保护为前提。

（二）欧盟破产程序中的数据权益

在欧盟法上，隐私权被视为一项基本人权，而数据权益被视为隐私权的延伸。[25]《欧盟基本权利宪章》（CFR）第 8 条第 1 款和《欧盟运行条约》（TFEU）第 16 条第 1 款几乎一致地规定“每个人都有权保护自己的个人数据”，欧盟法院（CJEU）同样承认保护数据的权利是一项基本权利。所以在欧盟法层面对于数据保护抱持高压态势，欧盟《通用数据保护条例》（General Data Protection Regulation，以下简称“GDPR”）也是在此观念前提下制定。作为欧盟的二级法律，GDPR 的适用必须确保“对自然人的基本权利和自由特别是隐私权的全面有效保护”[26]。对于欧盟破产程序中的数据权益保护问题，并无欧盟层面统一化的破产条例，所以应当具体结合成员国的破产法律进行观察。一般而言，GDPR 作为超主权的欧洲法律，其适用上的优先性高于成员国法律，如成员国破产法。这意味着，成员国破产法的原则与规则需要符合 GDPR 的要求，否则不得强制执行。下文将主要以德国法为例。

根据《德国基本法》第 1（1）条以及第 2（1）条的“人格自由发展权”，德国联邦宪法法院在 1983 年创造了个人数据自决权，这一判决被视为德国数据保护法之滥觞。[27] 德国法上，个人数据是人格之一部分，受制于“人是目的”这一先验认知的权威性和人权保护的神圣性，因此，作为人格构成部分的个人数据断不可成为受处分之客体。也就是说，如果债务人进入破产程序，个人数据是不得作为财产转让给第三人的。如果坚守这一人格保护的传统观念，个人数据的商品化利用不具可能，显然脱离现实发展的客观需要。为了缓解这种理论预设与实践应用上的冲突，学者指出，如果仅将视角放在个人数据是否可以转移，则会陷入人格权属性与财产权属性之间的法政策矛盾，应当避开这一途径，转而将个人数据权益与同其类似的权益进行类推比较，进而援用其规范，而对标的合适对象正是著作权。[28] 著作权与数据权益一样，不仅具有人格权益，也包含巨大的商业价值，虽然因人身专属而不能转让给第三方，但是可以在授权的基础上许可他人使用。根据著作权法原理，享有著作权的意义在于，他人未经许可不得以特定方式利用作品，所以是排他权而非自用权，[29] 类推至数据权益可得，只要数据主体许可他人使用数据，即可形成法律意义上的权益转让。

由上可知，德国法上的数据权益在破产程序中的转让存在解释上的可能性，若不能得到数据主体许可使用的意思表示，数据流转并无它途。此时，应进一步从 GDPR 的规则层面进行检验。

GDPR 第 6（1）条规定了 6 项数据处理合法事由。[30] 据此，除了数据主体的同意之外，尚

〔24〕 See In re Borders Groups，Inc.，No. 11－10614（Bankr. S. D. N. Y Sept. 27，2011).

〔25〕 See EU Agency for Fundamental Rights（FRA），Data Protection in the European Union：the Role of National Data Protection Authorities，[2010] 14.

〔26〕 Art. 7，8 of Charter of Fundamental Rights.

〔27〕 参见杨芳：《个人信息自决权理论及其检讨》，载《比较法研究》2015 年第 6 期；Ronny Hauck，Personal Data in Insolvency Proceedings：The Interface between the New General Data Protection Regulation and Insolvency Law，ECFR 2019：724，731.

〔28〕 参见前引〔27〕，Hauck 文，第 732 页。

〔29〕 参见前引〔14〕，王迁书，第 12 页。

〔30〕 译文主要参考瑞柏律师事务所译：《欧盟〈一般数据保护条例〉（汉英对照）》，法律出版社 2018 年版。

有其他可合法处理数据权益的特定事由，其中，第（3）项法律义务适用于法令或监管所施加的强制性要求，〔31〕第（4）项重大利益标准主要关乎自然人生命或其他人道主义利益，〔32〕第（5）项以公共利益为主，所以在破产程序语境下，如果仅考虑纯粹的市场化破产，则可能适用的合法事由只剩下为履行合同所必需与实现控制者或第三方所追求的合法利益。

在履行合同所必需的合法事由中，数据主体必须是待履行合同的当事方，或者，数据主体必须是为处理其数据所发起的合同之第三方受益人。欧洲数据保护委员会在对该条的指引中明确，进行“必要性”评估时，应当综合考虑网络行为广告、服务改进、私人定制、合同双方预期等，〔33〕数据主体的预期利益保护是必要性论证的核心，这直接显示出与目的限制的关联。换言之，破产程序中，除非数据主体在与数据控制者形成以数据为内容的法律关系时预期到，当数据控制者破产时会基于与交易对手的合同关系处理这些数据，否则该处理行为不应认为有效。这种对数据主体的过分期待已然有违数据主体的本意，因为数据主体在交付数据使用权时的合理期待一般是数据控制者稳健运营背景下的处理行为，而不应包括经营失败特别是破产时的出售行为，是故，该项合法事由在破产程序中的适用并不切实际。〔34〕

最后可能适用于破产程序中的数据处理合法事由是实现数据控制者或第三方合法利益所必需，这一事由越过了数据主体同意的要求，为执法机关提供了较大裁量权。根据立法说明，在数据主体未合理预期到数据将被进一步处理的情况下发生个人数据处理行为的，数据主体的利益和基本权利要优先于数据控制者的利益。〔35〕概言之，该合法事由本质上是利益衡量标准，需要对数据主体与数据控制者或第三人进行利益的平衡测试。对此，数据保护委员会的前身，也就是第 29 条工作小组曾细化过该指令所要综合考虑的因素，其中包括合法利益的性质与来源、对数据主体以及对数据处理之于合理预期的影响、是否有其他替代性保护措施如数据最小化、隐私增强技术等等。〔36〕破产程序中，一方是数据控制者与第三人对数据所附载商业价值的经济利益追求，另一方是数据主体的基本权利、基本自由等人格利益诉愿，形式上表现为数据自决权。在这两种利益之间进行权衡的司法与执法努力，显属不易，目前的实践尚未导出可一体适用的判例规则，是故，平衡的标准预期具有不确定性。〔37〕特别地，在 GDPR 第 83 条的罚款威慑下，破产管理人将个人数据作为有价资产进行出售的动力受到阻遏。由此决定了合法利益事由并不具有破产程序中数据处理的现实意义。

所以，在 GDPR 第 6（1）条规定的 6 项数据处理合法事由中，仍然是以数据主体的同意为黄金标准，除非获得数据主体的明确同意，否则破产程序中的数据权益出售将面临合法性质疑。

（三）小结

综上所述，破产程序中的数据保护思想渊源即个人控制论，在美国法上体现为公平信息实

〔31〕 See Peter Carey ed., *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, 2018, pp. 55 - 56.

〔32〕 See GDPR Recital (46)；前引〔31〕，Carey 书，第 56 页。

〔33〕 See EDPB: Guidelines 2/2019 on the Proceessing of Personal Data under Article 6 (1) (b).

〔34〕 参见前引〔27〕，Hauck 文，第 740 页。

〔35〕 See GDPR Recital (47).

〔36〕 See Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC, available at htttp://ec.europa.eu/justice/data-protection/index_en.htm, last visited on Jan. 19, 2022.

〔37〕 参见余佳楠：《个人信息作为企业资产》，载《环球法律评论》2020 年第 1 期；前引〔27〕，Hauck 文，第 742 页。

践，在欧盟法上表述为个人数据自决权。个人控制论是一项富含多元保护原则的价值体系，主要通过为数据主体赋权和施加数据控制者责任的方式保护数据主体的合理预期。〔38〕而在破产程序中，数据主体合理预期的稳定性被打破，围绕个体主义展开的风险防范制度必然以个人控制为核心，简言之，个人对数据的控制意愿决定了数据控制者进行数据处理的限度。

三、破产程序中个人控制论的困境与出路

个人控制论的预设前提是，数据主体具备充分理性并有能力权衡损益从而做出谨慎判断。然而在破产程序中，这一先验性的假设不仅高估了个体理性在数据关系中的可能性与必要性，也无法回应市场效率对于数据转让的客观要求。

首先，围绕个人控制的规则处于“主观上有控制意愿而客观上无控制可能”的尴尬境地，这在破产程序内外均属易见。数据主体的有限理性与认知不足，在相当程度上扭曲了个体在面对抉择时进行判断的成本收益结构，进而决定了个人控制无法保障数据主体在进行知情同意的选择之前已经展开充分的利益衡量。基于此，数据控制者通过利用并放大这种行为经济学意义上的不理性，以增加信息覆盖形成信息茧房、强化细节刻画制造阅读障碍，使得数据主体作出失真的判断。〔39〕一个典型的例子是，当数据主体在与数据控制者形成基于数据的法律关系时，很少特别留意后者所提供的隐私政策，仅仅是以便利使用为目的快速勾选同意条款，而忽视隐私政策中所涵括的涉及自身利益处置内容。此外，数据的算法处理被模糊为一种黑箱形态，导致回溯性证据获取几乎不可能，同时万物互联以企业之间的数据关联与共享为典型特征，当数据主体提交一份数据之后，多元化的信息融合令数据控制者身份复杂化和不易识别。〔40〕这都将限缩数据主体个人控制的成效。

其次，破产程序中的个人控制论无法回应市场效率对于数据转让的客观要求，根源上体现为与债务人财产价值最大化理念的冲突。破产法的立法目的在于扩充可供清偿的债务人财产，以集体性约束机制实现债权人公平受偿，〔41〕这就要求管理人或经管债务人在自动冻结程序开始之后尽可能地收集债务人财产。此时，数据的财产属性为破产债务人资产整理提供了财产法的理由，而数据的人格属性则限制了将数据作为交易所涉标的。数据主体与数据控制者及受让人之间的利益状态是不均衡的，个人控制论确有缓和、矫正这种不平等的作用，但其减弱了数据流通的合理频度和财产效度，抬高信息流通的成本，反而产生破坏性调整中的新一轮不平等状态。该种内在的冲突应由实定法的规则设计予以调整，而我国相关立法并未对此给予回应，进

〔38〕 参见丁晓东：《论个人信息法律保护的思想渊源与基本原理——基于“公平信息实践”的分析》，载《现代法学》2019 年第 3 期。

〔39〕 参见解正山：《数据驱动时代的数据隐私保护》，载《法商研究》2020 年第 2 期；John A. Rothchild, Against Notice and Choice: The Manifiest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else), 66 *Cleveland State Law Review* 559, 615 (2018).

〔40〕 See Daniel J. Solove, Introdution: Privacy Self-management and the Consent Dilema, 126 *Harvard Law Review* 1880, 1881 (2013).

〔41〕 参见前引〔5〕，Baird、Jackson 文，第 103 页。

一步加重了紧张关系。

从破产法的视角来看，个人控制对于数据的处理而言并不具有可欲性，如果强化个人控制，将衍生更多破产法上的难题。例如，在重整程序中，重整计划通过之前的“363 出售”一般要求在正常营业范围内，对于绝大多数非以数据处理为业务的企业而言，数据出售显然超出常规营业范围，而必须经过听证程序才能实现。〔42〕 如果听证程序中，数量庞大的数据主体利益代表人不同意出售方案，以“假马竞价”为基础所实现的趋向最大化资产出售目的将无法达成。另外，如果是按照常规的重整计划表决，基于数据享有权益的索取权人尚无法定依据成为具有法律地位的主体从而划入相应组别，即便法律为此提供了特别保护，现实中的操作也将类似于大规模证券代表诉讼一般复杂，程序参与成本奇高；如果将数据保护官（Data Protection Officer）作为代表人参与破产衍生诉讼，其所代表的权益比重界定将耗费更高的估测成本，反而与债务人财产最大化的目的背道而驰。

综上所述，个人控制论之于破产程序中的数据处理而言确有一定弊端。合适的方案应是对既有的讨论基础进行修正。传统数据保护的学理研究往往侧重个人与数据企业平台之间的对抗性状态，先验地推定后者对于前者权益的侵害，设置“通知—同意”规则可以降低这种侵害可能性。然而一味强调数据控制者会损害数据主体权益的观念，弱化了个人在与数据平台企业建立数据关系时所保有的信任，而且不利于数据控制者自行构建约束性规范、提高问责意识。

从卡拉布雷西与梅拉米德所构建的卡梅框架的角度进行解读，通过法律赋权并控制数据流动的个人控制论属于财产规则，〔43〕 而这一规则适用的核心问题在于行权障碍，特别是当数据主体与数据控制者存在实质上的权力地位不平等时，数据主体的行权成本将据此抬高。在破产程序中，要求数据主体根据数据控制者所提示的处理申请进行选择，其行权成本在于对可选方案进行量化评估和谨慎选择的识别成本，财产规则并不总是能够为数据主体提供妥善的保护。出路在于，当特定的情形发生时，压缩数据主体与数据控制者之间的协商空间，将其转化为半强制性的剥夺行为，并为该行为造成的负面效果提供补偿，是为责任规则。〔44〕 责任规则引入破产程序中的数据处理，其基本思路是将破产作为特定的事由，要求数据主体允许数据控制者为实现债务人财产最大化等目的处理个人数据，前提是数据控制者为此向数据主体提供充分的补偿。这一思路转向，将规范重点从数据控制者向数据主体请求授权，调整为当破产情事发生时，数据控制者应依循相关义务约束，并在违背义务时向数据主体负担法律上的责任，此时，义务约束内容是为数据主体的利益最大化服务，而法律责任则体现为因违反义务对数据主体承担的补偿性责任。

四、破产程序中数据权益保护的路径优化：信义义务论

必须承认，数据平台企业对于现代社会已经不可或缺，特别是 COVID-19 大流行等灾难性事

〔42〕 See 11 U. S. C. § 363.

〔43〕 See Guido Calabresi，Douglas Melamed，Property Rules，Liability Rules，and Inalienability：One View of the Cathedral，85 *Harvard Law Review* 1089，1092 (1972).

〔44〕 参见前引〔43〕，Guido Calabresi、Douglas Melamed 文，第 1092 页。

件更促进了在线生活的常态化。〔45〕由于数据主体与数据控制者之间的严重信息不对称，数据主体极易受到数据控制者的伤害，前者必须相信后者不会背叛其信任以操纵之。〔46〕从信任角度理解数据关系并为数据控制者施加更高的行为标准，成为对个人控制论理念弊端的有效补充。美国学者杰克·巴尔金等将信义法引入数据关系，认为数据主体基于其对数据控制者的信息不对称状态以及信任关系，从而形成信义关系，数据控制者对数据主体负有信义义务，并在违反义务条件下承担责任。〔47〕印度《个人数据保护法》第26条即引入了数据受托人概念，显示出学理与实践的互动。毫无疑问，这一观点为企业正常运行时数据控制者与数据主体之间的关系构造提出了新的解释，然而在企业破产时能否提供同样的解释力，并非不言自明。

需说明的是，将数据控制者界定为数据受托人的解释模糊了数据平台企业与其运营者之间的身份界定，如印度《个人数据保护法》中将数据受托人界定为“单独或与他人共同决定处理个人数据的目的和手段的任何人，包括邦、公司、任何法律实体或任何个人”〔48〕。在数据关系中，数据控制者通常指平台企业实体，而具体履行控制职能的则是以公司董事会及管理层（以下合称“董事会”或“董事”）为代表的企业内行政管理团队。本文一体使用这两个概念，因为当数据平台企业作为受托人时，本质上就是董事会履行受托人义务，易言之，当我们在说数据控制者的信义义务，实际上就是指董事的信义义务，下文也主要围绕董事的信义义务展开。而必要的区分在责任分配层面。

（一）破产程序中数据控制者信义义务的法理基础

传统公司法理论认为，在企业正常运营时，由于所有权与控制权的分离，执掌公司运营权力的董事与暂居消极角色的股东之间形成紧张关系，为避免紧张关系产生的代理成本挫伤公司绩效、损害股东利益，公司法规定董事应对股东/公司负担信义义务，〔49〕从而保证董事积极履职并维持忠诚。当企业破产时，为了防止董事懈怠必须为其行为提供清晰指引，比较法上进而发展出信义义务转化理论，即根据信托基金、风险负担等理论，认定信义义务受益人从股东转向债权人。〔50〕然而这一转化理论似乎并不能够为数据主体的利益保护提供同等适用空间，因为，数据关系的定性并不能从债之关系加以把握。换言之，当企业进入破产时，数据主体具有特殊的法律地位，除非法律作了例外规定，否则信义义务转化理论无用武之地。事实上，这一争论的焦点在企业正常运营时便存在，如针对巴尔金的数据信义义务理论，美国反垄断新星丽娜·蒽便结合特拉华州公司法的立场认为数据关系中的信义义务将使董事面临在股东与数据主体之间利益权衡的两难。〔51〕这一问题在破产程序中更为突出。

---

〔45〕 See Yan Xiao, Ziyang Fan, 10 Technology Trends to Watch in the COVID-19 Pandemic, WORLD ECON. F. (Apr. 27, 2020), available at https://www.weforum.org/agenda/2020/04/10-technology-trends-coronavirus-covid19-pandemic-robotics-telehealth, last visited on Jan. 19, 2022.

〔46〕 See Jack M. Balkin, The Fiduciary Model of Privacy, 134 *Harvard Law Review* 11 (2020).

〔47〕 See Jack M. Balkin, Information Fiduciaries and the First Amendment, 49 *U. C. Davis Law Review* 1183 (2016).

〔48〕 印度《个人数据保护法》第2（B）（13）条。

〔49〕 See Stephen Bainbridge, *Corporate Law*, Foundation Press, 2015, p. 113.

〔50〕 参见陈鸣：《董事信义义务转化的法律构造——以美国判例法为研究中心》，载《比较法研究》2017年第5期。

〔51〕 See Lina M. Khan, David E. Pozen, A Skeptical View of Information Fiduciaries, 133 *Harvard Law Review* 497 (2019).

证成数据控制者对数据主体的信义义务主要有两种路径，第一种是基于信义义务存在的实质条件，亦即，无论所处情事如何，只要满足信义义务认定的基本要求，即可承认信义义务存在，这也被称为构成要件理论；第二种是限于破产这一特定情形，从既有的理论资源中寻找信义义务涵括数据关系的可能性，笔者认为合适的理论资源是团队生产理论。以下分而述之。

1. 信义义务构成要件理论

通常而言，信义关系是信任、信心、信赖的多重结合关系，受益人将其对于特定事项的控制权转移至受托人，以期待受托人基于受益人的利益而行使权利。〔52〕塔玛·芙兰珂（Tamar Frankel）教授将信义关系构成要件归结为四项：首先，受托人所提供的主要是劳务服务（相对于商品而言），且其所提供之劳务服务内容，在一般社会观念之期待下，须具备一定专业技能，如提供医疗、法律、公司经营管理等；其次，为能有效提供前述劳务，受托人必须被赋予具有处理财产或授予权利之权限；再次，委托人须负担受托人有无法安全被信赖之风险，意即受托人可能会有违背职务或滥用权限之行为，或无法依所承诺之服务内容适当履行；最后，存在三项风险，（1）委托人在信义关系中，无法为适当之自我保护，（2）市场机制也无法对委托人之风险提供保障，（3）受托人如果要取信委托人，可能必须付出高于其可自信义关系所获利益之成本。〔53〕这一构成要件理论已深获学界认许。〔54〕

破产程序中数据控制者与数据主体之间是典型的信义关系。数据主体基于对数据控制者专业能力和职业操守的信任，将数据提交给控制者，在破产程序中所固定的数据承载着用户的原始期待；数据控制者在企业运行稳健时提供相对应的数字化服务，在破产程序中则根据可能的技术化条件延续或优化服务内容。这一服务在一般社会观念下具有专业性、技术性，数据控制者对于该数据行使相当程度的处理权限，而数据主体无从通过有效的市场机制对控制者行为进行约束，数据控制者滥用权力或怠于提供服务并以牺牲数据主体数据权益为代价增进自身利益的可能性抬升。此时必须借助强有力的私法保护机制约束数据控制者的行为，也就是信义义务规则。

2. 破产程序中的团队生产理论

团队生产理论起源于经济学上对生产团队与企业绩效关系的研究，其核心内容是囿于团队成员投入与最终产出之间对应关系的不确定性，将剩余索取权人列为团队监督者有利于实现有效激励。〔55〕公司法学者将其引入公司分析中，指出公司是由不同的参与人为了共同的利益而组成的一个生产团体，各种参与人贡献不同但是地位一样，比如股东出金钱，董事出管理，雇员出劳力等，为了准确地衡量并分配生产绩效，应将独立的董事会制度视为协调性科层安排（mediating hierarchy），进而最大限度鼓励并保证每一位主体均进行资产专用性投资、锁定资本，而向团队

〔52〕 See Lawrence Mitchell, Fairness and Trust in Corporate Law, 43 *Duke Law Journal* 425, 430 (1993).

〔53〕 See Tamar Frankel, *Fiduciary Law*, Oxford University Press, 2010, pp. 4 - 6.

〔54〕 See Andrew S. Gold, Paul B. Miller, *Philosophical Foundation of Fiduciary Law*, Oxford University Press, 2016, pp. 1 - 17.

〔55〕 See Armen A. Alchian, Harold Demsetz, Production, Information Cost and Economic Organization, 62 *American Economic Review* 777 (1972).

成员负担信义义务是董事履职的重要前提。〔56〕循此思路，数据主体将数据提交给平台企业，从而成为企业生产团队之一员，并与雇员、股东等享受同样的保护，董事对数据主体负担信义义务属于团队生产理论应有之义。

进入破产重整程序，学者发展出重整中的团队生产理论，在这一框架下，团队成员在重整之前成立公司时的契约继续有效，团队成员基本上仍然保留下来参与重整，团队内部的各个成员将以重整程序为博弈空间，从而对团队契约进行一定程度的修正，为了避免团队成员协商的无效率，该理论认为应由董事会代表团队修正该契约。〔57〕这一理论建构与重整程序中的债务人经管模式相一致，具有解释力。其中，为避免董事会修正团队契约过程消极懈怠或以权谋私，该理论强调应要求其继续负担对团队成员的信义义务。〔58〕以此为前提，破产重整程序中，数据主体同样依据其投入数据的原始行动而成为团队生产合同的一员，并享有团队权利，数据主体在缺乏特别的保护机制下，无力对抗其他强势权利人如优先级债权人等，所以由董事会居中协调并履行对团队成员的信义义务，将最大限度地保护各类主体权益。

综合两种学说可以发现，尽管数据主体并非债权人，无法用信义义务转化理论加以涵摄，但其因对数据存有期待性法益，可借助信义义务构成要件理论与团队生产理论加以证成。

（二）我国破产程序中数据控制者信义义务的实施机制

英美法上，往往以对衡平法益的保护在个案中阐释信义义务，数字平台畛域内要求增加信义义务的适用已经成为英美学界的主流取态，在破产程序中引入数据控制者的信义义务虽尚无判例法实践，但其符合适用语境，可在个案中激活。我国并无衡平法传统，也缺乏个案造法的司法权力，对实施机制的探寻则须另觅他路。

我国《企业破产法》第27条规定了破产管理人应当勤勉尽责，忠实执行职务，但并未对债务人自行经管情形下管理层的信义义务进行说明。前述构成要件理论和团队生产理论均为管理层对数据主体负担信义义务提供了观念资源，实证法应对此做出响应。换言之，在破产法修改之际，创设一部信息时代的破产法的目标决定了应当将对数据主体的保护纳入考虑范围，信义义务是为有益的制定法尝试。不过，我国《民法典》第7条规定的诚实信用原则，因在本质上与信义义务内容相当，〔59〕均指向对不忠行为与懈怠行为的管制，在现阶段足为破产程序中董事的信义义务提供规范依据。《个人信息保护法》第5—9条从限制欺诈、合理目的、透明化、准确性、保密与安全等方面对个人数据处理行为设定了原则化要求，从所欲规范的行为而言，均与信义义务相符。司法层面，应遵循以上要求探索可供识别的标准，准确对应现实需求。首先，应尝试建立数据受托人的定义性规范，以便在破产程序中清晰地判定责任主体，关键问题在于是否任何涉及数据处理的企业均应负担类似信义义务，或是否应根据数据平台企业的体量进行分类规制。这不

〔56〕 See Margaret M. Blair, Lynn A. Stout, A Team Production Theory of Corporate Law, 85 *Virginia Law Review* 247, 248－257 (1999).

〔57〕 See Lynn M. LoPucki, A Team Production Theory of Bankruptcy Reorganization, 57 *Vanderbilt Law Review* 741 (2004).

〔58〕 参见前引〔57〕，LoPucki文，第741页。

〔59〕 参见楼建波、姜雪莲：《信义义务的法理研究——兼论大陆法系国家信托法与其他法律中信义义务规则的互动》，载《社会科学》2017年第1期。

仅取决于技术化时代企业的发展态势，更应结合反垄断等竞争性法律对相关平台企业地位的界定。尽管尚无确信的指引，但显而易见，在破产程序中，超级网络平台自然须负担更高标准的信义义务。其次，须明确合理期待标准具体指什么。与侵权法上的注意义务所承担的角色一样，合理期待标准决定了是否构成义务违反。注意义务是行为人的主观状态并通过具体行为予以客观化。细化合理期待标准，则不仅需要明晰企业正常运营时数据主体的期待可能，还应给定破产程序中数据主体的期待利益，将二者加以比较，甚至可以综合多项因素建立量化模型，测试是否违反信义义务。

（三）破产程序中数据控制者信义义务的内容构成

信义义务二元论是信义法理论的基石，即以忠实义务保证受托人在面临利益冲突时舍弃自身利益，以注意义务要求受托人在知情的基础上勤勉尽职。〔60〕破产程序中的数据权益处理，数据主体对数据平台企业的依赖性更强，而且对于数据平台企业所可能采取的危害行为控制力更弱，〔61〕是故，对数据控制者信义义务的要求也随之提升。信义义务是一个开放的体系，具有伸缩的概念禀赋，能够适应不同语境呈现更为丰富的内涵。

首先，应当将注意义务内容扩充为保密义务与安全义务。注意义务以知情判断为前提，从而勤勉尽职，敦促经营管理层采取合规手段保证内部信息传输系统高效完备，为谨慎的商业判断提供条件。然而在破产程序中，涉及数据处理时，知情判断已非主要诉求，数据主体对平台企业的合理期待中包含着数据保密与数据安全的内容，而这两项均可以在注意义务的文义解释范围内导出。注意，或者谨慎，主要指以一种方式行事或言谈以避免引起冒犯或暴露私人数据的品质，〔62〕保密是最有力的注意形式，它确保受托人必须在有限的范围内共享信息，并维持信任。〔63〕破产程序中，对数据权益的处理可能涉及多重复制、传输，有泄密的风险，谨慎的保密义务要求受托人保证其处理数据的行为特别是接受数据的第三方是值得信赖的，〔64〕在技术上可要求受托人采取措施保证通过搜索引擎乃至非法的爬虫等途径无从获得该类数据。安全义务与保密义务是一体两面，它进一步抬升了保护标准，将是否采用安全保障提高到是否采用符合行业标准或用户合理期待的程度。这一保护标准要求，根据用户数据的性质、质量、浓度等作出区分性和同一性保护，即同等数据同等保护，不同数据分类保护。在此项下，还须遵循适应性原则，即根据当前技术的发展水平和企业本身所能承受的成本约束等加以适应性的动态调整，如引入 K -匿名、差分隐私等越来越成熟的技术减少重新识别的风险。〔65〕保密义务与安全义务的设置有利于数据主体信任受托人在破产程序中不危害自身，确保接收数据的下游是合法的适格买受人，从而放心大胆地将个人数据交付后者而非进行持续性监督成本投入，避免数据泄露产生的风险与焦虑以及对人

〔60〕 参见前引〔49〕，Bainbridge 书，第 113 页；前引〔53〕，Frankel 书，第 52 页。

〔61〕 参见前引〔47〕，Balkin 文，第 1222 页。

〔62〕 See Discretion，Oxford English Dictionaries，available at http://www.oxforddictionaries.com/us/definition/american_english/discretion，last visited on Jan.19，2022.

〔63〕 See Neil Richards，Woodrow Hartzog，Taking Trust Seriously in Privacy Law，19 *Stanford Technology Law Review* 431，460 (2016).

〔64〕 参见前引〔63〕，Richards、Hartzog 文，第 461 - 462 页。

〔65〕 See Felix T. Wu，Defining Privacy and Utility in Data Sets，84 *University of Colorado Law Review* 1117 (2013).

格权益的损害。

其次，受托人应履行持续披露义务以实现透明性要求。当事人的有效谈判是破产程序特别是重整的灵魂，但是当事人自发谈判不等于有效谈判，其容易陷入囚徒困境，从而产生损人不利己的结果。〔66〕学理上，破产程序中持续披露的意义一方面在于引导当事人展开有效谈判，另一方面则通过当事人异议制度和灵活务实的披露内容设计，令信息披露更契合当事人表决的需要。〔67〕如前所述，尽管在个人控制论的视角下，在破产程序中持续性地披露数据处理细节，可能并不能够令数据主体采取行动以保障自身数据安全，但是披露行为本身可以使数据主体感到信赖，正如论者所言，“通过披露行为传递的信任信号，比收集数据时反复允诺不会随意与第三方公司共享的模糊保证，更为直观而实用”〔68〕。进而引出的问题是披露信息的内容与强度为何。应当认为，根据比例原则，披露的内容主要限于非商业秘密以及非加工后的数据，亦即仅仅针对数据主体而言具有保护必要性的数据。此外，在披露过程中应采取手段防范数据主体的恶意利用和非法反向工程，防止部分主体借破产程序推进之名，行盗用数据牟取非法利益之实。至于披露的程度，不应要求令所有数据主体完全了解数据处理细节，而只需要符合基本的商业规范或行业要求，可借鉴证券法上的真实、准确、完整标准。换言之，只要披露行为依循合理的操作规程，满足用户的信赖保护需求，即可认为透明性信义内容的实现。

最后，受托人须履行忠实义务以实现数据主体利益最大化。忠实义务是信义义务的核心，它奠定了数据关系中数据控制者不作恶的理论基础。破产程序中，受托人所面临的利益冲突尤甚，如果在破产程序中面临董事利益与团队生产中其他成员的利益冲突，董事自保的动机可能会促使牺牲其他成员的权益，其中就包括数据主体权益。忠实义务为受托人行为确立了明确的指引，在面临利益冲突时，必须以维护包括数据主体权益在内的团队权益为目的。忠实义务并不意味着受托人不获取利益，〔69〕而是要求受托人必须进行利益衡量，将数据主体权益置于自身利益之上。例言之，如果在破产程序推进过程中，受托人违背隐私政策与第三方共享数据、根据数据主体类型在维权层面的能力差异歧视性地捏软柿子、通过不当的信息提示误导数据主体选择次优的利益处置方案等，均将构成对忠实义务之违反。

（四）破产程序中数据控制者违反义务的责任分配

前述关于数据受托人的责任讨论，是从宽泛的视角论证责任承担的条件，在实践中，有必要进一步分析数据平台企业与董事会之间的责任分配。在破产程序中，可能存在的责任分配类型是：（1）数据平台企业单独承担责任；（2）数据平台企业与董事共同承担责任。两种责任分配方式的主要区分在于董事承担连带责任情形。根据学界主流观点，即对于数据保护的规范学说，场景化识别与规制是构建数据保护法律关系的重要原则，亦即，根据场景化分类谨慎识别行为属性

〔66〕 参见高丝敏：《重整计划强裁规则的误读与重释》，载《中外法学》2018 年第 1 期。

〔67〕 参见高丝敏：《论破产重整中信息披露制度的建构》，载《山西大学学报（哲学社会科学版）》2021 年第 3 期。

〔68〕 前引〔63〕，Richards、Hartzog 文，第 464 页。

〔69〕 参见前引〔47〕，Balkin 文，第 1225 页。

并加以控制。〔70〕当前，数据外包产业的迅速发展，〔71〕推动形成企业自建数据分析系统与企业外包数据服务两种场景。〔72〕

第一种场景，大型数据平台企业自行研发智能化机器进行数据分析。此时，进入破产程序，董事会应当负总责。责任分配应具体化为以下情形：第一，董事会若积极监督系统是否符合安全标准，以信义义务为指引，谨慎地在推进破产程序中改善、调整数据处理所需的安全技术环境，此时，如若发生数据损害，经过具有行业标准化水平和资质的第三方专业技术机构鉴定发现最终的不利后果由数据分析系统本身的故障所产生，且该故障非可由董事履职所能排除，则认其对最终的数据损害不具有可归责性，应由公司按照破产程序中的正常风险承担责任；第二，如果董事未能确保履职过程中达到信义义务标准、满足用户合理期待，产生了最终的损害后果，且数据分析系统并无设计上的故障，纯粹因董事行为失误所致，董事应当对此结果与公司承担连带赔偿责任。至于董事承担责任的形态应当是仅由技术背景董事担责还是与其他非技术背景董事共同承担连带责任，这一问题与数据处理事项对专业化系统的依赖程度、破产事件对数据处理造成的影响力度、技术董事的解释必要性与清晰度等等因素有关，应根据特定案情加以厘定，不应设定一刀切的规范基准，否则将损及破产程序中董事的行动预期。

第二种场景下，第三方提供数据外包服务。此际，虽然数据外包企业进行数据分析处理，但仍然以董事会指示为依据，两者之间的关系可比照电子代理人行为，令前者行为归诸董事会。〔73〕关键在于，数据外包企业会基于其成熟的数据处理经验，在破产程序中为董事会提供备选处理方案。在此模式下，首先，如果董事会对于数据外包企业提供的处理方案进行了技术层面的审查，如复盘和检测了记录数据处理过程的相应分析步骤，在保证其符合安全和保密性要求时，可视为已经适当履职，对于最终的数据泄露风险，应由公司承受。其次，如果董事会在未进行合理审查的条件下，误信数据外包公司的处理建议，从而导致数据损害，则需与公司承担连带责任。至于对数据外包公司的追偿，则由二者之间的合同关系加以调整。

五、结　论

通过信义义务为破产程序中数据权益提供实质性保护，与个人控制论的数据保护立场形成合力支撑的体系效用。企业破产对数据保护场景的调整决定了数据主体合理期待应受到更高标准和更为细化的延续，避免数据主体负载在数据之上的人格权益与财产权益的流失。对数据控制者施以信义义务的法定性标准，能在畅通数据财产权益流转和维护数据人格权益正当性之间获得平

〔70〕 See Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford University Press, 2010, pp. 1 - 11. 相关中文介绍，参见前引〔8〕，丁晓东文。

〔71〕 See Pierangela Samarati, Sabrina De Capitani di Cimercati, Data Protection in Outsourcing Scenarios: Issunes and Directions, ASIACCS' 10: Proceedings of the 5th ACM Symposium in Information, Computer and Communications Security, April 2010 Page 1 - 14, available at http://doi.org/10.1145/1755688.1755690, last visited on Jan. 19, 2022.

〔72〕 参见程威：《人工智能介入董事会的董事义务与责任更新》，载《东北大学学报（社会科学版）》2022 年第 2 期。

〔73〕 参见高丝敏：《智能投资顾问模式中的主体识别与义务设定》，载《法学研究》2018 年第 5 期。

衡。具体承担信义义务的董事会应与数据平台企业一同负担信义义务，并通过责任约束确保数据主体的合理期待得以满足。我国现行法对信义义务的认知仍有不足，仅通过诚信义务的知识体系提供类似保护固然有益，但仍缺乏信义义务的实质性判定规则。在《个人信息保护法》施行和即将启动的《破产法》修改过程中，应当注意数据控制者在破产程序中履行信义义务的内容，探讨适度追究数据控制者违反义务的责任，在破产程序中创造更为有效的数据主体权益的保护制度。

Abstract: The protection of data rights and interests in the bankruptcy procedure has been paid more and more attention, but the current applicable rules of real right, contract and intellectual property are facing the dilemma of insufficient protection and improper adjustment. The standpoint of personal cybernetics established by comparative law, from the perspective of data subject locking the direction of data use, restricts the commercialization of data rights too much, fails to adjust the internal conflict between data personality rights and property rights, and is inconsistent with the concept of maximizing the value of debtor's property in the bankruptcy procedure. Should pay attention to the establishment of trust relationship between the data subject and the data controller, based on faith obligations constitutive requirements theory and team production theory in bankruptcy law, apply confidentiality, security, transparency and faithful trustee obligations for the data controller in the bankruptcy proceedings, and properly allocate responsibility according to the path of scenario in a data platform between the enterprise and business management. Through the mandatory legal liability constraint, it provides the behavior guidance for the data controller in the bankruptcy procedure, so as to strengthen the protection of the rights and interests of the data subject in the bankruptcy procedure.

Key Words: data equity, data controller, fiduciary duty, team production theory, scenario-based regulation

（责任编辑：周　游　赵建蕊）

财经法学 No. 6，2022
pp. 65 - 80

互联网不正当竞争类型化条款司法适用的反思与纠正

黄　军*

内容提要：互联网不正当竞争类型化条款在制度供给层面顺应了互联网领域竞争行为的规制需求。该类型化条款在司法运行层面主要有“独立适用”“二元并存适用”“三元混合适用”三种模式。司法实践中，现有类型化条款在规范适用结构上面临“泛化”与“虚化”困境，在规范适用逻辑关系上呈现明显对立性，在规范适用构成要件解析上缺乏一致性。寻求互联网不正当竞争类型化条款司法适用的优化可从三方面着手：一是通过明确兜底条文适用解释的同质性、厘清列举条款适用对象的指向性以及凸显宣示条款适用功能的区分性，明晰不同规范适用的具体定位；二是采取“二元协作评价路径”以厘定类型化条款与一般条款的外部逻辑关系；三是构建起“前置的竞争关系＋合法的竞争利益＋特定的竞争行为＋多元的竞争损害＋合理的竞争抗辩”的统一规范要件适用程式。

关键词：反不正当竞争法　互联网不正当竞争　类型化条款　一般条款

一、引　言

近些年随着互联网领域竞争日趋白热化，各类新型不正当竞争行为层出不穷，基于对旧法一般条款在实践中日渐凸显的不确定性问题的内在省思与深入检讨，尤其是及时回应由此引发的“向一般条款逃逸”现象的普遍关切，〔1〕在广泛梳理、归纳与总结既有典型案例基础上，立法者通过2017年《反不正当竞争法》修订之机最终确立了互联网不正当竞争类型化条款（即第12

* 黄军，青岛大学法学院讲师。

〔1〕 参见陈兵：《互联网经济下重读“竞争关系”在反不正当竞争法上的意义——以京、沪、粤法院2000—2018年的相关案件为引证》，载《法学》2019年第7期。

条)。在规范构造层面，除了具有浓厚倡导意味的第 1 款规定（即宣示条款）以外，现有类型化条款采取了“概括＋列举＋兜底”的复合体例。

从立法初衷与功能指向维度来看，作为修法中的“形象工程”，互联网不正当竞争类型化条款不仅象征着互联网时代的“标杆条款”，〔2〕也在制度供给层面顺应了互联网领域竞争行为的规制需求。在条款颁行前后，学界就此展开了广泛讨论，但更多侧重从法解释学进路对条文构造及其意涵加以考察与剖析。问题在于，书本上的法不等于行动中的法，对法律真正科学的描述一般认为，法律殊非书面上的文字所言——“法律即所作为”。〔3〕进一步而言，“虽然法提出的主要是一种规范性要求，但法律之治却必须基于坚实的实证基础之上，否则法律之治的目标就可能会落空”〔4〕。依此检视，围绕互联网不正当竞争类型化条款的既有研究成果不仅呈现出明显的同质化取向，〔5〕而且针对规范的运行效果也未给予必要且足够的理论关照。鉴于此，本文采取实证化分析进路，通过梳理司法案例具体考察现有类型化条款的适用模式，探究其在实践中面临的突出问题，最终提出相应的改进建议。

二、互联网不正当竞争类型化条款司法适用的不同模式

（一）独立适用模式

独立适用系指法院主要援引第 12 条规定作为审理互联网不正当竞争案件的实体裁判依据，不涉及反不正当竞争法其他具体规制条款。其可一分为二：

1. 整体适用

整体适用是法院在个案中对互联网不正当竞争类型化条款未加以具体筛选，而选择一体化适用进路以判定涉案行为是否构成不正当竞争。其包括两种形态：一是直接型整体适用，在“奇虎与搜狗不正当竞争纠纷案”〔6〕“聪明狗与淘宝不正当竞争纠纷案”〔7〕以及“百度与搜狗不正当竞争纠纷案”〔8〕中，法院在明确援引第 12 条基础上分别对竞争行为正当性作出界定；二是间接型整体适用，在由北京知识产权法院审理的“迪火与三快不正当竞争纠纷案”〔9〕中，法院基于条文逻辑关系考量后指出，被诉行为已经违反第 12 条，对于是否违反第 2 条规定不再评述，故最终主要依据互联网不正当竞争类型化条款作出了相应判决。

2. 局部适用

局部适用是在具体分解第 12 条规定内部体系构造基础上，结合个案情形仅援引互联网不正

〔2〕 参见孔祥俊：《反不正当竞争法新原理·分论》，法律出版社 2019 年版，第 528－529 页。

〔3〕 参见〔美〕萨默斯：《美国实用工具主义法学》，柯华庆译，中国法制出版社 2010 年版，第 107 页。

〔4〕 罗豪才、宋功德：《软法亦法——公共治理呼唤软法之治》，法律出版社 2009 年版，第 67 页。

〔5〕 涉及互联网不正当竞争类型化条款的代表性文献主要有：李扬：《互联网领域新型不正当竞争行为类型化之困境及其法律适用》，载《知识产权》2017 年第 9 期；孔祥俊：《论新修订〈反不正当竞争法〉的时代精神》，载《东方法学》2018 年第 1 期；郑友德、王活涛：《新修订反不正当竞争法的顶层设计与实施中的疑难问题探讨》，载《知识产权》2018 年第 1 期；蒋舸：《〈反不正当竞争法〉网络条款的反思与解释——以类型化原理为中心》，载《中外法学》2019 年第 1 期。

〔6〕 参见北京市海淀区人民法院（2016）京 0108 民初 14003 号民事判决书。

〔7〕 参见北京知识产权法院（2019）京 73 民终 1128 号民事判决书。

〔8〕 参见北京市海淀区人民法院（2017）京 0108 民初 7967 号民事判决书。

〔9〕 参见北京知识产权法院（2018）京 73 民初 960 号民事判决书。

当竞争类型化条款中具有指向性的特定条文。其可一分为三：

一是单独适用第 12 条第 2 款第 2 项。在“百度与乐活不正当竞争纠纷案”〔10〕中，法院认为，被告针对原告搜索服务的页面图片宣传屏蔽广告和新闻的功能，并屏蔽了原告的产品服务和付费搜索广告结果，因而认定其违反了第 12 条第 2 款第 2 项。

二是独立适用第 12 条第 2 款第 4 项规定。〔11〕例如在“优酷与视客不正当竞争纠纷案”中，法院指出，针对通过视客 App 便可免费完整获取优酷公司的视频播放服务的行为，鉴于其在外形上无法被纳入第 12 条第 2 款前三项所明定的互联网不正当竞争之情形，因而最终认定应由第 12 条第 2 款第 4 项调整。

三是共同适用第 12 条第 1 款与第 2 款第 1 项规定，或者共同适用第 12 条第 1 款与第 2 款第 4 项规定。在“百度与搜狗不正当竞争纠纷案”〔12〕中，针对被告通过技术手段导致在其浏览器地址栏中输入原告目标网址或者更改浏览器主页设置或者设置标签页均会跳转为被告导航网址的行为，法院同时援引第 12 条第 1 款与第 2 款第 1 项规定作出了判决。在“优酷与徐州百狐网不正当竞争纠纷案”〔13〕“爱奇艺与乐播不正当竞争纠纷案”〔14〕“腾讯与微源码不正当竞争纠纷案”〔15〕“优酷与锋芒不正当竞争纠纷案”〔16〕以及“腾讯与谌洪涛等不正当竞争纠纷案”〔17〕中，法院认定涉案竞争行为构成第 12 条第 2 款第 4 项之情形，且在裁判依据中一并提及第 12 条第 1 款与第 2 款第 4 项。此种模式中，法院虽述及第 12 条第 1 款，但真正发挥实质性调整作用的仍为列举条款。

（二）二元并存适用模式

二元并存适用是法院既援引了互联网不正当竞争类型化条款，也适用了反不正当竞争法或者其他法律中的实体规制条款作为共同的审理依据。其大致涉及如下情形：

1. 与一般条款的共同适用

一是形式意义上的共同适用，即法院在界定涉案竞争行为正当性时优先参照具体条款，但最终仍于裁判依据中同步列明第 2 条与第 12 条。此种情形下，判定涉案行为是否构成不正当竞争时，发挥独立评价作用的规范依据为第 12 条，第 2 条仅居于辅助性地位。详细而言，前述“辅助性地位”有如下具体表现：（1）合法权益证成。在“优酷与百度不正当竞争纠纷案”〔18〕中，法院结合对第 2 条的意涵阐释与个案事实的综合衡量，认可原告享有反不正当竞争法保护之利

〔10〕 参见北京市海淀区人民法院（2018）京 0108 民初 38881 号民事判决书。

〔11〕 相关案例参见北京知识产权法院（2020）京 73 民终 49 号民事判决书；北京市海淀区人民法院（2019）京 0108 民初 34763 号民事判决书；北京市海淀区人民法院（2018）京 0108 民初 2065 号民事判决书；北京市海淀区人民法院（2019）京 0108 民初 51116 号民事判决书；广东省广州市天河区人民法院（2019）粤 0106 民初 40045 号民事判决书；北京知识产权法院（2020）京 73 民终 1556 号民事判决书；上海市徐汇区人民法院（2018）沪 0104 民初 243 号民事判决书；北京市海淀区人民法院（2017）京 0108 民初 36596 号民事判决书；北京市海淀区人民法院（2017）京 0108 民初 24512 号民事判决书；江苏省高级人民法院（2019）苏民终 778 号民事判决书。

〔12〕 参见北京市海淀区人民法院（2018）京 0108 民初 42023 号民事判决书。

〔13〕 参见北京市海淀区人民法院（2017）京 0108 民初 54830 号民事判决书。

〔14〕 参见北京市海淀区人民法院（2018）京 0108 民初 48523 号民事判决书。

〔15〕 参见广东省深圳市中级人民法院（2017）粤 03 民初 773 号民事判决书。

〔16〕 参见北京市海淀区人民法院（2019）京 0108 民初 28000 号民事判决书。

〔17〕 参见上海市浦东新区人民法院（2019）沪 0115 民初 73840 号民事判决书。

〔18〕 参见北京市海淀区人民法院（2017）京 0108 民初 57274 号民事判决书。

益。(2) 竞争关系厘定。在“复娱与微梦不正当竞争纠纷案”〔19〕中，法院借助对第 2 条规定的意涵推衍，确认原被告双方存在竞争关系。(3) 规范关系阐明。在“前锦与逸橙不正当竞争纠纷案”〔20〕中，法院重申了最高人民法院在“海带配额案”中所确立的独立适用第 2 条的基本要件，进而释明了一般条款与具体条款之间的相互关系。

二是实质层面上的共同适用，即裁判依据中同时引用了第 2 条与第 12 条，且各自发挥了规制效力。其包括如下类型：(1) 针对同一竞争行为，同时适用第 2 条与第 12 条进行评价。〔21〕在“腾讯与通路、云电、罗博特等系列不正当竞争纠纷案”中，法院认为，涉案微信群控系统对微信平台争取到的用户注意力和交易机会造成了破坏和损害，明显不符合诚信原则，有违第 2 条规定；同时法院提到，前述干扰行为也违反了第 12 条规定。(2) 针对不同行为，分别适用第 2 条与第 12 条进行评价。在“猎豹、金山与二三四五不正当竞争纠纷案”〔22〕中，法院指出，被告擅自变更网络用户浏览器主页的行为属于第 12 条规定的误导、欺骗、强迫用户修改、关闭原告合法提供的网络产品的情形；至于涉案区别对待行为，法院认为，其违背了第 2 条规定的自愿、平等、公平、诚信的原则，有悖于法律和商业道德。

2. 与其他具体条款的共同适用

在“金豪风机与金河风机不正当竞争纠纷案”〔23〕中，法院在分析论证与裁判依据部分依次引用了第 6 条与第 12 条，但最终因原告举证不足而驳回了其诉讼请求。在“福州神康医院与平潭精神病防治院不正当竞争纠纷案”〔24〕中，一审法院指出，被告在搜索引擎上设置与原告名称相关的信息等作为关键词不仅足以误导公众，也妨碍了原告提供的网络服务正常运行，故根据第 6 条与第 12 条规定确认其构成两类不正当竞争行为。在“神马与搜狗不正当竞争纠纷案”〔25〕中，法院借助第 8 条与第 12 条分别针对搜狗的虚假宣传、遮挡浏览器输入法增强栏和设置搜索候选词误导用户进入搜狗搜索的竞争行为作出了否定性评价。

3. 与《商标法》条文的共同适用

在“快手与易智侵害商标权纠纷案”〔26〕中，法院援引《商标法》第 57 条第 1 项、第 2 项认定被告涉案软件使用与涉案商标相同或近似的标识，侵害了原告享有的注册商标专用权；针对被告在原告经营的 App 中强制进行目标跳转的行为，法院结合《反不正当竞争法》第 12 条第 2 款第 1 项规定判定其构成不正当竞争。

4. 与《著作权法》条文的共同适用

在“腾讯与点云侵害作品信息网络传播权系列纠纷案”〔27〕中，法院认为，点云公司未经授

〔19〕 参见北京知识产权法院 (2019) 京 73 民终 2799 号民事判决书。

〔20〕 参见上海知识产权法院 (2019) 沪 73 民终 263 号民事判决书。

〔21〕 相关案例参见杭州铁路运输法院 (2019) 浙 8601 民初 1661 号民事判决书；重庆市第五中级人民法院 (2019) 渝 05 民初 3618 号民事判决书；天津市第一中级人民法院 (2019) 津 01 民初 1319 号民事判决书；浙江省高级人民法院 (2020) 浙民终 330 号民事判决书；广东省深圳市中级人民法院 (2019) 粤 03 民初 1911 号民事判决书；广东省深圳市中级人民法院 (2019) 粤 03 民初 1912 号民事判决书；广东省深圳市中级人民法院 (2019) 粤 03 民初 1913 号民事判决书。

〔22〕 参见上海知识产权法院 (2019) 沪 73 民终 241 号民事判决书。

〔23〕 参见山东省沂源县人民法院 (2020) 鲁 0323 民初 473 号民事判决书。

〔24〕 参见福建省高级人民法院 (2020) 闽民终 554 号民事判决书。

〔25〕 参见北京市海淀区人民法院 (2016) 京 0108 民初 16044 号民事判决书。

〔26〕 参见北京市海淀区人民法院 (2018) 京 0108 民初 68074 号民事判决书。

〔27〕 参见杭州互联网法院 (2020) 浙 0192 民初 1329 号民事判决书；杭州互联网法院 (2020) 浙 0192 民初 1330 号民事判决书。

权将涉案游戏置于其云服务器中供公众在移动端、web 端以及 PC 端使用“菜鸡”云游戏平台获得其提供的涉案游戏之行为，违反了《著作权法》第 48 条第 1 项规定，侵害了原告享有的信息网络传播权；并进一步判定点云公司限制涉案游戏外部链接跳转功能已妨碍、破坏了原告合法提供的涉案游戏正常运行，违反《反不正当竞争法》第 12 条第 2 款第 4 项规定。

5. 与《合同法》条文的共同适用

在“爱奇艺与龙境不正当竞争纠纷案”〔28〕中，法院指出，涉案分时出租 VIP 账号行为有违原被告双方关于 VIP 账号使用权限的约定，且双方约定未违反《合同法》关于格式条款无效之规定，因而该行为不具有正当性；针对被告通过技术手段对涉案爱奇艺 APP 部分功能加以限制的行为，法院认定其违反了《反不正当竞争法》第 12 条规定，并进一步提到，在已适用具体条款情形下，不再支持原告关于同时适用该法第 2 条进行调整的主张。

（三）三元混合适用模式

此处的三元混合适用，系指法院在实践中援引了涵括《反不正当竞争法》中的互联网不正当竞争类型化条款在内的三类规制条文作为实质性裁判依据之情形。

1. 与一般条款、误导性宣传规制条款的共同适用

在“腾讯与微时空不正当竞争纠纷案”〔29〕中，其裁判依据主要涉及《反不正当竞争法》第 2 条第 2 款与第 3 款、第 8 条第 2 款、第 12 条第 1 款与第 2 款第 4 项。析言之，法院通过援引第 2 条中有关经营者的规定，指出涉案原被告之间面临着直接的竞争利益冲突，故认定其构成反不正当竞争法意义上的竞争关系；在具体引述第 8 条第 2 款条文前提下，法院基于案件事实判定被告为他人提供微信软件刷量服务行为符合“帮助他人虚假宣传”的行为构成；同时，法院认为，前述有偿刷量服务行为属于第 12 条第 2 款所规制的“妨碍、破坏网络产品或者服务正常运行”的不正当竞争行为。

2. 与一般条款、商业秘密规制条款的共同适用

在由杭州市中级人民法院审理的“迪火与三快不正当竞争纠纷案”〔30〕中，最终判决的规则指引主要涉及《反不正当竞争法》第 2 条、第 9 条以及第 12 条。首先，法院基于迪火公司的涉案命名规则不符合商业秘密构成中的秘密性要求，未支持有关被告违反第 9 条的侵权指控；其次，针对原告主张被告实施具有“控制/干扰/中断”原告系统的行为，法院经过分析后认定，其不违反第 12 条；最后，法院认定被告行为未有违反诚实信用原则或公认的商业道德，不损害反不正当竞争法所保护的法益，并不违反第 2 条规定。

3. 与一般条款、商业诋毁规制条款的共同适用

在“金山与二三四五不正当竞争纠纷案”〔31〕中，法院采用的裁判依据主要包括第 2 条第 1 款与第 2 款、第 11 条、第 12 条第 2 款第 2 项。首先，法院认定，被告的涉案行为属利用技术手段，通过影响用户选择，误导、欺骗用户修改、关闭其他经营者合法提供的网络产品或者服务，

〔28〕 参见北京市海淀区人民法院（2018）京 0108 民初 37522 号民事判决书。
〔29〕 参见广东省深圳市中级人民法院（2019）粤 03 民初 594 号民事判决书。
〔30〕 参见浙江省杭州市中级人民法院（2018）浙 01 民初 3166 号民事判决书。
〔31〕 参见上海市浦东新区人民法院（2018）沪 0115 民初 62506 号民事判决书。

构成不正当竞争；其次，法院指出，被告在弹窗中对原告的涉案描述行为构成商业诋毁；最后，法院认为，被告实施的区别对待行为有违诚实信用原则与平等竞争原则，与商业道德背道而驰，扰乱了市场竞争秩序，损害了原告的合法权益，构成不正当竞争。

三、互联网不正当竞争类型化条款司法适用中存在的问题

（一）规范适用结构面临“泛化”与“虚化”困境

1. 兜底条文的泛化适用

泛化适用系指法院依据互联网不正当竞争类型化条款中的兜底条文来处理相关案件时，因缺乏对现有规范构成要件的清晰厘定与合理限缩，导致出现不当的扩展适用甚至明显的滥用情形。究其缘由，发生泛化适用与兜底条文所固有的不确定性密切相关。在互联网领域竞争形态日新月异背景下，竞争行为无可避免会呈现变异性与多样性，仅借助具有鲜明阶段性与指向性的列举条文无法实现对不正当竞争行为的周延规制，此时引入具有概括性与可解释性的兜底性规定殊为必要。问题在于，既有兜底条文的文本表述显得过于宽泛，规范内涵与外延具有高度不确定性。其主要体现为：如何理解其中的“正常”运行，是采用技术标准，还是法律标准；如何确定认定主体，以及举证责任；何谓作为对立的不正常、失常或者异常情形；等等。〔32〕由此导致的后果是，依据互联网不正当竞争类型化条款来评价互联网竞争行为时，兜底条文很可能负担“不可承受之重”，甚至可能将正当竞争行为贴上不正当竞争“标签”。〔33〕结合司法实践层面而言，此种泛化适用现象得到了不同维度的具体体现。

从形式上来看，此种泛化最为直观地反映为作为审理依据的兜底条文在相关案件中呈现出的居高不下的引用比重。这某种程度上也反映出法院在处理此类纠纷时存在明显的路径依赖。就实质层面而言，泛化适用突出表现为法院未能科学且准确地把握规范的核心要义，在适用兜底条文时采取过于宽松的解释态度，试图“一兜了之”，使得该类型化条款的规制效力出现不合理的溢出效应，逾越应有的调整界限。在备受关注的视频广告屏蔽领域，尽管学界围绕该行为的法律属性界定存有“不正当性说”〔34〕“正当性说”〔35〕与“折中说”〔36〕等观点，但新法颁行后不少法院在审理相关案件时开始纷纷由一般条款转向适用互联网不正当竞争类型化条款中的兜底条文，进而认定其构成不正当竞争。前述“优酷与视客不正当竞争纠纷案”便为具例。在法理意义上，“法律规则可适用于某一案件事实，意味着该案件事实能够归属于该法律规则构成要件所指陈的事实类型”〔37〕。依此审视既有裁判，一个被忽略的基础性问题在于：视频广告屏蔽行为虽在外观

〔32〕 参见前引〔5〕，郑友德、王活涛文。

〔33〕 参见张占江：《论反不正当竞争法的谦抑性》，载《法学》2019 年第 3 期。

〔34〕 参见宋亚辉：《网络干扰行为的竞争法规制——“非公益必要不干扰原则”的检讨与修正》，载《法商研究》2017 年第 4 期。

〔35〕 参见王迁：《论规制视频广告屏蔽行为的正当性——与“接触控制措施”的版权法保护相类比》，载《华东政法大学学报》2020 年第 3 期。

〔36〕 参见周樨平：《竞争法视野中互联网不当干扰行为的判断标准——兼评“非公益必要不干扰原则”》，载《法学》2015 年第 5 期。

〔37〕 黄泽敏：《法律漏洞填补的司法论证》，载《法学研究》2020 年第 6 期，第 64 页。

上初步契合了“其他妨碍、破坏”竞争行为的基本构成，但从体系解释维度而言，由于现有类型化条款中与之最为近似的干扰行为（即误导、欺骗、强迫类）须以违背用户意愿作为前置限定，其与视频广告屏蔽行为顺应用户需求之间迥然有别，如此一来，屏蔽行为便不应被直接纳入互联网不正当竞争类型化条款中兜底条文的规制框架之中。〔38〕通过以上简要分析，兜底条文在具体实践中的泛化适用情形可见一斑。

2. 其他规则的虚化适用

虚化适用是指互联网不正当竞争类型化条款中兜底条文以外的其他规范在个案中无法发挥出实质意义上的法律拘束力，处于虚化运行状态。其主要包括如下两种情形：

一是宣示条款徒具象征意义。在现有判决文书中，虽有部分案件的裁判依据直接述及这一条文，但往往仅是作为一项套路式的附带表述。以前述“腾讯与微时空不正当竞争纠纷案”为例，在认定涉案行为正当性时，法院分别援引第 2 条、第 8 条第 2 款以及第 12 条第 2 款，第 12 条第 1 款仅是突兀地出现在最终裁判依据之中，该规则适用背后的内在逻辑与理据基础并未得到必要阐释。这样一来，第 12 条第 1 款实则陷入“可有可无”的尴尬境地。

二是列举条款面临规制乏力困境。尽管互联网不正当竞争类型化条款中列举条款是立法者通过典型案例归纳，进而抽象与提炼出互联网新型不正当竞争共性行为要素的产物，但缺陷在于，现有规定的行为构成过于具化，而个案情形却十分复杂，仅具一时情景性的具体规则显然难以达致应有的普适性，这势必对其法律适用造成不小的困扰。〔39〕

（二）规范适用逻辑关系呈现明显对立性

1. 规范内部适用的形式逻辑矛盾

规范内部适用的形式逻辑矛盾是指不同法院根据互联网不正当竞争类型化条款来认定同一涉案互联网竞争行为时得出不同的法律结论，即“同案不同判”。这可借助前述由两地法院审理的“迪火与三快不正当竞争纠纷案”的相反判决得到直接例证。杭州市中级人民法院指出，三快公司没有主动、强行在二维火收银系统中插入链接，仅是向用户提供了选项，由用户自行进行选择，无证据表明在安装或运行过程中存在“误导、欺骗、强迫”用户的行为，最终认定不构成《反不正当竞争法》第 12 条规定的不正当竞争行为。与之相反，北京知识产权法院则认为，涉案行为违反了第 12 条第 2 款第 1 项与第 4 项规定。显然，前述做法不符合法律规范适用应当遵循的一致性规则，也有违用于衡量司法公正的“同案同判”原则。〔40〕

2. 规范外部适用的形式逻辑矛盾

规范外部适用形式逻辑矛盾是指法院援引互联网不正当竞争类型化条款（主要指向兜底条款）审理案件时，围绕涉案竞争行为是否需要同时引入一般条款的评价机制及其具体作用发挥程度方面存有不小分歧。其具体体现为三种不同意见：

一是单一评价路径，即仅依据互联网不正当竞争类型化条款来判定涉案互联网竞争行为的正当性，排除一般条款具有的调整空间。以“爱奇艺与龙境不正当竞争纠纷案”为例，法院指出，鉴于

〔38〕 参见前引〔5〕，蒋舸文。

〔39〕 参见刘维：《论软件干扰行为的竞争法规制——基于裁判模式的观察》，载《法商研究》2018 年第 4 期。

〔40〕 参见孙海波：《“同案同判”：并非虚构的法治神话》，载《法学家》2019 年第 5 期。

被诉行为已适用《反不正当竞争法》第 12 条，对于同时适用该法第 2 条进行调整的主张不再支持。

二是二元协作评价路径，即在适用互联网不正当竞争类型化条款来评价涉案竞争正当性情形时，主张引入一般条款加以共同认定。例如，在“腾讯与点云侵害作品信息网络传播权系列纠纷案”中，法院指出，在适用《反不正当竞争法》第 12 条第 2 款第 4 项时要结合该法一般条款的构成元素和判断范式进行具体认定。

三是二元独立评价路径，即判断涉案互联网竞争行为正当性时，主张独立运用互联网不正当竞争类型化条款与一般条款进行双重评价。例如，在“腾讯与硕文不正当竞争纠纷案”中，法院指出，被告研发并提供具有屏蔽（拦截）视频及贴片广告的涉案软件行为违反了诚实信用原则和公认的商业道德，属于《反不正当竞争法》第 2 条及第 12 条规定的不正当竞争行为。

（三）规范适用构成要件解析缺乏一致性

当前不同法院针对互联网不正当竞争类型化条款的规范适用构成要件缺乏相对一致的标准。其主要有如下不同主张：

1. 二要件构造说

法院将互联网不正当竞争类型化条款的适用构成区分为两大部分的观点具体如下：（1）“技术手段”＋“妨碍行为”。在“快乐阳光与搜狗不正当竞争纠纷案”中，法院指出，《反不正当竞争法》第 12 条第 2 款规定的适用要件包括：利用技术手段实施行为；妨碍、破坏其他经营者合法提供的网络产品或服务的正常运行。（2）“妨碍行为”＋“主观故意”。在“优酷与千影不正当竞争纠纷案”中，一审法院认为，被诉行为客观上破坏了原告合法提供的网络服务，且主观具有恶意，构成《反不正当竞争法》第 12 条第 2 款第 4 项规定的不正当竞争。（3）“客观行为”＋“损害后果”。在“腾讯与数推不正当竞争纠纷案”中，法院指出，被诉行为是否违反《反不正当竞争法》第 12 条规定可从两方面分析：是否符合该条规定的不正当竞争行为特征；是否损害社会公共利益，损害互联网经营者、用户和消费者的合法权益。（4）“权益受保护性”＋“行为不当性”。在“爱奇艺与龙境不正当竞争纠纷案”中，一审法院认为，判断被诉行为是否构成《反不正当竞争法》第 12 条规定的不正当竞争主要涉及两方面：原告是否享有受反不正当竞争法调整的权益；被诉行为是否属于网络环境下的不当行为。

2. 三要件构造说

该观点将互联网不正当竞争类型化条款的适用构成分解为三项要件，具体解读如下：（1）“技术手段”＋“妨碍结果”＋“违反诚信原则与商业道德”。在“爱奇艺、众源与千影不正当竞争纠纷案”中，一审法院指出，适用《反不正当竞争法》第 12 条第 2 款第 4 项规定应满足如下条件：使用技术手段影响用户选择或直接替代用户选择；导致其他经营者合法提供的网络产品或服务不能正常运行；有违自愿、平等、公平、诚实信用的原则与公认的商业道德。（2）“经营行为的合法性与正当性”＋“技术手段”＋“妨碍后果”。在“优酷与百度不正当竞争纠纷案”“优酷与乐播不正当竞争纠纷案”以及“优酷与视客不正当竞争纠纷案”中，法院适用《反不正当竞争法》第 12 条第 2 款规定认定涉案竞争行为正当性时，均将其细化为：原告提供的网络服务正当、合法；被诉行为利用技术手段实现；妨碍、破坏了原告网络服务的正常运行。（3）“竞争关系”＋“主观过错”＋“损害后果”。在“追风与京东不正当竞争纠纷案”中，二审法院阐明了《反不正当

竞争法》第 12 条第 1 款的三个适用要件：存在竞争关系；具有主观故意；造成损害后果。

3. 四要件构造说

该观点认为互联网不正当竞争类型化条款的适用构成牵涉四项要素，主要表述如下：(1)“经营者合法权益受损”＋“损害消费者利益”＋“行为不当性”＋“市场秩序损害”。在“腾讯关于微信群控系统与通路、云电、罗博特等系列不正当竞争纠纷案”中，法院认为，适用《反不正当竞争法》第 12 条第 2 款第 4 项规定需从四个方面进行分析：其他经营者合法权益受损；采用技术手段损害了消费者利益；违反诚信原则和公认的商业道德；破坏了互联网环境中公平竞争的市场秩序。(2)“竞争关系”＋“技术手段”＋“主观过错”＋“行为不正当性”。在“腾讯与点云侵害作品信息网络传播权系列纠纷案”中，法院在论证原被告存有竞争关系（基于业务与用户的交叉重合标准）基础上，进一步阐述了《反不正当竞争法案》第 12 条第 2 款第 4 项规定的适用要件：在技术角度，妨碍、破坏行为针对权利人本身；存在主观过错；涉案竞争行为具有不正当性和可责性。(3)“合法权益”＋“主观过错”＋“妨碍行为”＋“损害后果”。在“猎豹、金山与二三四五不正当竞争纠纷案”中，法院认为《反不正当竞争法》第 12 条第 2 款第 2 项规定的适用要件包括：原告经营产品具有合法性；利用技术手段的故意性；实施了相关妨碍行为；影响了原告提供的合法网络产品。(4)“竞争关系”＋“技术手段”＋“妨碍行为”＋“损害后果”。在“腾讯与微时空不正当竞争纠纷案”中，法院适用《反不正当竞争法》第 12 条第 2 款规定时着重考量了如下因素：界定竞争关系（采纳竞争利益冲突标准）；使用技术手段；实施妨碍行为；造成损害后果（包括扰乱市场竞争秩序与损害原告合法权益）。

4. 五要件构造说

该说主张互联网不正当竞争类型化条款的适用涉及“竞争关系”“技术手段”“主观过错”“行为可责性”以及“损害后果”五要件。在“爱奇艺与龙境不正当竞争纠纷案”中，二审法院认为，判断涉案行为是否构成不正当竞争，需要分析如下五项因素：是否存在竞争关系（主张在新经济模式下可从双方具体经营行为、最终利益存在竞争关系维度加以广义界定）；采取技术手段；主观过错；行为具有可责性；不当夺取交易机会或损害其他经营者合法利益。

综上所述，法院在个案中针对互联网不正当竞争类型化条款适用构成要件的解析虽有重叠之处，但也呈现出各自的内容侧重与表述差异，缺乏一致性。在此情形下，前述规范适用要件标准的不统一性不仅会引致不正当竞争认定标准的不确定性，也会不同程度地影响其规范指引功能的有效发挥。〔41〕

四、互联网不正当竞争类型化条款司法适用的改进路径

（一）明晰不同规范适用的具体定位

1. 明确兜底条文适用解释的同质性

适用解释的同质性，意在要求法院在审理互联网不正当竞争纠纷时应当通过引入与依循规范

〔41〕 参见黄武双、谭宇航：《不正当竞争判断标准研究》，载《知识产权》2020 年第 10 期。

解释层面的同质性规则，实现对具有高度不确定性的兜底条文的适度限制。所谓“同质性解释”，也称“相同类别解释规则”，是“在用特别的词描述一个种类或类别的人或事之后，如果紧接着使用了总括性的词，则该总括性语词只限于与特定的词所表达的同类的人或事”〔42〕。有此主张主要基于如下考量：首先，法律规范文本离不开相应的语境，探求兜底条文的具体意涵不应忽视对现有互联网不正当竞争类型化条款的规范语境进行分析，以尽可能达致对相关规范的语义还原与澄清〔43〕。其次，为了避免对互联网不正当竞争类型化条款的理解出现分歧甚至自相矛盾的局面，有必要运用体系性解释方法，即“先查清在若干法规范有意义的结合中清晰显现出来的类型的‘主导形象’，然后由此出发来解释个别规范”〔44〕。最后，囿于例示规定所能提供信息的有限性，兜底条款的明晰化往往有赖于立法意旨的具体化。〔45〕就互联网不正当竞争类型化条款中的兜底条款而言，其形式上的生成机理虽可归结于弥补列举立法体例难以穷举的固有缺陷，但理解实质意涵则需要借助对规范整体中其他规则的目的揭示来综合把握。

进一步而言，兜底条文适用解释同质性主要涵括两方面内容：一是基于列举条款的同质性解释规则，即在考察现有列举条款中的不正当竞争类型表现后，若认定涉案互联网竞争行为能够彰显前述相关类型的“意义联结”，便可初步将之视为兜底条文的调整对象；反之，便应将之排除在兜底条文的调整范域之外。〔46〕二是基于概括条款的同质性解释，即借助现有概括条款所提供的有关互联网不正当竞争行为定义中的“共通性构成”以指导兜底条文的适用解释。当然，前述两项同质性解释规则之间是相互联系、相辅相成的。析言之，根据列举条款的同质性解释规则来判断涉案情形是否属于兜底条款调整时，应以契合概括条款的本质意涵作为基本出发点与根本落脚点；在按照概括条款的同质性解释规则来界定个案是否适用兜底条款时，列举条款所具有的类型特质无疑可对其提供重要的认知指引。

2. 厘清列举条款适用对象的指向性

针对前述“列举条款规制乏力”问题，当前紧迫的任务是在正视既有规范不足基础上借助解释论路径阐明各项类型化规则意涵的具体指向，激活其规制效力。

针对规制插入链接与强制进行目标跳转行为的第 12 条第 2 款第 1 项规定，其明晰重点在于“意愿违背”与“行为表现”。就前者而言，现有规定针对“意愿违背”仅明确“未经其他经营者同意”，而缺少消费者意愿考量，这无疑有待商榷。设想某一跳转行为虽未经其他经营者同意，但顺应了用户的普遍意愿，此时将其认定为不正当竞争明显与互联网时代消费者所享有的主体性地位不符。〔47〕较为科学的解释应当是要求同时违背经营者与消费者的意愿。对此，2022 年颁行的《最高人民法院关于适用〈中华人民共和国反不正当竞争法〉若干问题的解释》第 21 条第 1 款作出了明确规定。〔48〕就后者而言，现有条文也未明确界定“插入链接”与“强制进行目标跳

〔42〕〔英〕约翰·格雷：《法律人拉丁语手册（双语版）》，张利宾译，法律出版社 2009 年版，第 58 页。

〔43〕参见刘继峰：《反不正当竞争法中“一定影响”的语义澄清与意义验证》，载《中国法学》2020 年第 4 期。

〔44〕〔德〕卡尔·拉伦茨：《法学方法论》，黄家镇译，商务印书馆 2020 年版，第 587 页。

〔45〕参见黄茂荣：《法学方法与现代民法》（第五版），法律出版社 2007 年版，第 191 页。

〔46〕参见李军：《兜底条款中同质性解释规则的适用困境与目的解释之补足》，载《环球法律评论》2019 年第 4 期。

〔47〕参见李海舰等：《互联网思维与传统企业再造》，载《中国工业经济》2014 年第 10 期。

〔48〕该解释第 21 条第 1 款规定：“未经其他经营者和用户同意而直接发生的目标跳转，人民法院应当认定为反不正当竞争法第十二条第二款第一项规定的‘强制进行目标跳转’。”

转”的逻辑关系，即究竟两者是并列关系，还是递进关系，抑或是重叠关系。在本文看来，结合司法实践采取相对灵活的解释策略可能更契合立法本意。

针对规制误导欺骗与强迫类行为的第 12 条第 2 款第 2 项规定，其解释重点在于“行为方式”与“侵害对象”。就前者而言，现有条款要求相关主体实施有关“误导、欺骗、强迫”行为。三者既可以构成独立关系，也可以形成交叉关系。在实质意涵方面，判定“误导”的关键在于“是否如实反映商品或服务的客观情况，是否造成用户的误解并产生不适当的联想”；“欺骗”则强调对用户采取了虚构事实、隐瞒真相的做法；“强迫”意在揭示通过“野蛮行为”直接侵害消费者的选择自由与决定自由。〔49〕就后者而言，修改、关闭、卸载他人提供的网络产品或者服务，其隐含的前提是用户已经安装相关产品或者接受相关服务，因而该条文所规定的行为侵害对象应仅限于已经获得的网络产品或服务。

针对规制恶意不兼容行为的第 12 条第 2 款第 3 项规定，除了需界定主观意味浓重的“恶意”以外，该条文与《反垄断法》相关条款的关系协调问题亦亟需厘清。理论而言，恶意不兼容行为既可能构成滥用市场支配地位行为或者垄断协议行为，也可能构成互联网不正当竞争行为，因而针对该行为的规制可能适用反垄断法，也可能适用反不正当竞争法。这就意味着，当涉案不兼容行为经初步形式判定落入反垄断法的适用范围时，便应由反垄断法进行规制，而非由反不正当竞争法调整。〔50〕概言之，互联网不正当竞争类型化条款所禁止的不兼容行为指向的是垄断行为以外的行为。

3. 凸显宣示条款适用功能的区分性

凸显宣示条款适用功能的区分性旨在充分发挥该条款之于互联网不正当竞争行为所具有的分流规制作用，即互联网不正当竞争类型化条款“仅规定互联网领域的特殊行为，传统不正当竞争行为在互联网领域的延伸部分，适用相应的条款调整”〔51〕。事实上，此举也有利于及时纠正实践中出现的不当援引互联网不正当竞争类型化条款来处理传统不正当竞争行为的错误做法。例如，在“福州神康医院与平潭精神病防治院不正当竞争纠纷案”中，尽管该案发生于互联网领域，带有互联网因素，但涉案行为（使用他人企业名称作为关键词进行的网络宣传推广行为）本质上与传统的商业混淆行为并无二致。此时，不能仅凭借助互联网平台实施争议行为所依托的实施环境、发布媒体等背景差异选择转向互联网不正当竞争类型化条款的规制路径。〔52〕

（二）厘定类型化条款与一般条款的逻辑关系

厘清类型化条款与一般条款之逻辑关系，旨在化解互联网不正当竞争类型化条款适用中出现的规范外部适用的形式逻辑矛盾。本文主张，今后法院在处理互联网不正当竞争类型化条款与一般条款关系时应当采取“二元协作评价路径”，理由在于：一方面，将一般条款与具体条款结合加以适用的做法不仅能够满足人们对于法秩序的确定性需求，也能使法院在未来实践中创制相应的具体规则，确保法律规范具有足够的生命力。〔53〕另一方面，这是有效克服互联网不正当竞争

〔49〕 参见谢兰芳：《论互联网不正当竞争中消费者利益的保护》，载《知识产权》2015 年第 11 期。

〔50〕 参见前引〔5〕，蒋舸文。

〔51〕 前引〔2〕，孔祥俊书，第 531 页。

〔52〕 参见曹丽萍、张璇：《网络不正当竞争纠纷相关问题研究——〈反不正当竞争法〉类型化条款与一般条款适用难点探析》，载《法律适用》2017 年第 1 期。

〔53〕 参见〔奥〕恩斯特·A. 克莱默：《法律方法论》，周万里译，法律出版社 2019 年版，第 43 页。

类型化条款逻辑缺陷及其解释难题的必然选择。其中现有类型化条款的逻辑缺陷主要体现为规范设置的“非互斥性”与“非周延性”。前者表征的是列举条款所涉的互联网不正当竞争行为类型之间构成交叉重叠关系，而非应然层面的互斥关系，故可能导致同一行为被不同列举条款所共同涵括；后者是指列举条款针对互联网不正当竞争行为的类型归纳有限，无法有效覆盖其他典型的不正当竞争行为形态，诸如“不当抓取他人数据行为”。〔54〕现有类型化条款的解释困境源于规则本身具有的抽象性与模糊性，这不仅体现在规范构造方面，也反映在具体条文较为含糊的概念表述之中。〔55〕前述类型化条款中的逻辑缺陷与解释难题不仅会极大降低规则在实践中的适用性与操作性，也会诱发相关互联网不正当竞争案件变成“临界案件”〔56〕甚至“疑难案件”〔57〕之风险。在此背景下，通过引入更具涵括性与本质性的一般条款的综合分析，将成为处理此类不正当竞争纠纷的合理选择。

在个案中，根据具体规范选取的不同，此种“二元协作评价路径”实际上将包括“弱二元协作评价”与“强二元协作评价”两种形式。析言之，当对涉案互联网竞争行为表现进行考察后，初步得出结论其应当援引的裁判依据为互联网不正当竞争类型化条款中的列举条款，但由于缺乏对相关规范适用构成要素的清晰界定，为了避免法律适用过程中可能出现的滥用与误用等异化情形，法院虽有必要结合一般条款对涉案行为加以共同评价，但鉴于列举条款所描述的行为类型指向相对明确，故一般条款的引入更多是检验类型化条款的具体适用是否有违其所确立的正当性判定的基本标准。不难看出，此种“弱二元协作评价”得以采纳应当符合如下前提限定：一是个案情形在外观上符合列举条款所规定的行为特征，需纳入列举条款的规制范围；二是法院就涉案情形适用列举条款时对相关规范构成适用要素存疑。而在行为评价的具体作用方面，一般条款所发挥的主要是一种相对较弱的辅助论证功能。相较而言，当法院认定涉案事实可落入互联网不正当竞争类型化条款中的兜底条文时，囿于该规定针对不正当竞争行为的构成要件并不完整，此时便有必要结合一般条款来对涉案行为的法律属性进行界定。采取“强二元协作评价”的原因主要在于个案中所援用的规则指向兜底条文，但其无法提供有效的不正当竞争认定标准。而在评价作用定位层面，一般条款的引入将会在实质层面发挥出较为独立的补充评价效力。

（三）构建统一的规范要件适用程式

为了避免互联网不正当竞争类型化条款适用中出现前述的内部形式逻辑矛盾，殊有必要构建一套一致性的规范适用程式，以实现互联网不正当竞争认定标准与裁判结果的双重统一。

1. 前置的竞争关系

“前置的竞争关系”旨在肯定竞争关系之于互联网不正当竞争认定所具有的前提限定价值。在个案中，法院应当坚持审查是否存在竞争关系，将其作为适用互联网不正当竞争类型化条款的

〔54〕 相关典型案件可参见由北京市海淀区人民法院审理的“抖音诉刷宝不正当竞争纠纷案”与“新浪微博诉超级星饭团不正当竞争纠纷案”。

〔55〕 参见黄军：《视频网站商业模式竞争法保护的反思与完善》，载《时代法学》2019 年第 3 期。

〔56〕 “临界案件”是就某一案件是否可被纳入相关法律条文的涵摄范围存在争议。参见杨仁寿：《法学方法论》（第二版），中国政法大学出版社 2013 年版，第 113 页。

〔57〕 疑难案件是指在法律的理解与适用方面存在争议的案件。参见孙海波：《不存在疑难案件?》，载《法制与社会发展》2017 年第 4 期。

先决条件。当经过初步分析后判定原被告双方有竞争关系时，不正当竞争认定便进入下一环节；反之，则随即终止。理据在于：首先，不正当竞争行为的本质为竞争行为，而竞争行为是一种相对性行为，即行为发生于竞争对手之间，这就意味着不正当竞争只能存在于竞争者之间。〔58〕互联网不正当竞争行为无出其外。其次，基于互联网经济对传统竞争模式的颠覆进而否定竞争关系之于行为正当性的前提要件意义，是对竞争关系相对性的误读。尽管泛诸互联网领域的跨界竞争不同于以往传统行业的直接竞争，但从根本上看，其竞争的目的仍在于努力获得另一个人同时也在努力获得的东西，〔59〕这一过程并未脱离基本的竞争关系框架。最后，梳理域外同类立法安排与司法实践后不难发现，主要国家（德国与美国）在规范经营者之间的竞争秩序时，通常也未放弃考察竞争关系因素。〔60〕当然，在理解互联网领域的竞争关系时，有必要结合这一领域的行业分工日趋细化、业务交叉重合逐渐盛行的既有现实，采取相对宽泛的阐释。

2. 合法的竞争利益

一方面，《反不正当竞争法》第 12 条将互联网不正当竞争行为的侵害客体规定为“其他经营者合法提供的网络产品或者服务”，实则已经蕴含立法者对于“合法的竞争利益要素”的明确要求；另一方面，法院运用互联网不正当竞争类型化条款来处理此类纠纷时，往往也会重视对原告合法竞争利益的具体分析。

当然在个案中分析合法竞争利益要素时，应当避免陷入如下误区：一是泛化合法竞争利益。原告享有的合法竞争利益是有具体指向的，且可被直接证实，不能将整个互联网行业所集聚或者形成的共有利益直接归于个体的竞争利益。例如，将存在于互联网视频领域“免费＋广告”商业模式所产生的竞争利益等同于特定经营者享有的竞争利益便有待斟酌。二是固化合法竞争利益。竞争机制是一种优胜劣汰的效能竞争机制，竞争者应当依靠优质优价的产品或者服务（即经营活动业绩与优势）开展有效竞争。〔61〕当互联网领域出现新的竞争业态并逐渐取代旧竞争业态时，新的竞争利益势必会对既有的竞争利益构成根本威胁与挑战，基于前述效能竞争理论考量，此时便不应继续坚持对原有竞争利益的固化保护，而应强调竞争利益的动态性与可更迭性。

3. 特定的竞争行为

在现有规范框架下，法院适用互联网不正当竞争类型化条款来判断涉案竞争行为正当性时，需要立足于如下几个方面进行体系化考量。

一是行为手段的技术性，即互联网不正当竞争是“利用技术手段”实施的。在个案中判定是否使用技术手段方面，除了技术特征较为明显的情形以外，本文认为，对于疑难复杂案件可采取“反向推定＋举证否定”的分析方法，即原告或者法院基于相关互联网专业人士的分析意见得出“非由技术手段而无法实现”判断时，除非被告通过举证证明未采用技术手段，否则应当作出肯定式结论。

二是行为方式的影响性，即互联网不正当竞争必须是通过“影响用户选择或者其他方式”实

〔58〕 参见焦海涛：《不正当竞争行为认定中的实用主义批判》，载《中国法学》2017 年第 1 期。

〔59〕 参见〔英〕哈耶克：《个人主义与经济秩序》，邓正来译，复旦大学出版社 2012 年版，第 106 页。

〔60〕 参见前引〔41〕，黄武双、谭宇航文。

〔61〕 参见郑友德、范长军：《反不正当竞争法一般条款具体化研究——兼论〈中华人民共和国反不正当竞争法〉的完善》，载《法商研究》2005 年第 5 期。

现。其中“影响用户选择”含义相对明晰；“其他方式”则主要指向的是“影响经营者经营”。因为就行为指向而言，某一互联网不正当竞争行为不是针对相关用户，便是针对市场上其他经营者的经营活动。〔62〕

三是行为表现的多样性。互联网不正当竞争类型化条款将该语境下不正当竞争行为的表现形式概括为“妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为”，即网络干扰行为。当然由于兜底条文的设置，也就保留了互联网不正当竞争表现形式的其他可能性。

四是行为过错的明显性。依据现有规范文本，互联网不正当竞争类型化条款所涉的不正当竞争行为的主观过错包含故意与一般过失及以上的形态，两者均具有明显性。因为就保护对象而言，互联网不正当竞争类型化条款保护的并非法定权利，而是成熟度较低的利益。这样一来，只有当明显违反相关领域中需要遵守的注意义务、存在明显过错时，方可认定构成不正当竞争，否则便有可能引致市场行为动辄得咎、过度限制自由竞争的消极后果。〔63〕

4. 多元的竞争损害

虽然现有类型化条款将互联网不正当竞争的形式损害表述为“妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行”，但实质的利益受损形式则可从不同维度进行把握。

一是直接意义上的竞争利益受损。在适用互联网不正当竞争类型化条款时，首要的利益衡量在于考察个案中相关经营者的竞争利益受损情形，尤为需要注意以下方面：在损害对象方面，其既有可能是初始的竞争利益损害，也有可能涉及衍生的利益损害。在损害程度方面，其既涵括相对轻微的损害形式——“妨碍”，也牵涉较为严重的损害后果——“破坏”。前者是指互联网不正当竞争虽然导致他人网络产品或者服务造成阻碍，但仍可运行；后者则是导致他人的网络产品或者服务直接陷于瘫痪或者部分功能受损。〔64〕在损害发生状态方面，其既包含现实发生的损害，也涉及可能发生的损害。

二是独立意义上的消费者利益受损。随着反不正当竞争法由传统向现代的转变，消费者利益作为不正当竞争认定的一项独立考量因素的重要性日渐凸显。〔65〕事实上，“在用户为王、消费者主导市场经济发展风向标的互联网时代，消费者居于市场竞争法的核心，消费者利益一改既有的依附地位，成为反不正当竞争法的直接保护法益”〔66〕。结合 2022 年《最高人民法院关于适用〈中华人民共和国反不正当竞争法〉若干问题的解释》来看，这样一种转变也得到了直接体现。〔67〕就互联网不正当竞争类型化条款的司法适用而言，在根据消费者利益受损情况来认定涉案行为正当性时，其具体的考量内容虽牵涉消费者的知情权、隐私权以及选择权等不同方面，〔68〕

〔62〕 事实上，早先的《反不正当竞争法（修订草案送审稿）》与《反不正当竞争法（送审稿）》中，“影响用户选择”与“干扰其他经营者正常经营”也是并列呈现的。

〔63〕 参见王文敏：《反不正当竞争法中过错的地位及适用》，载《法律科学》2021 年第 2 期。

〔64〕 参见焦海涛：《互联网不兼容行为的规制路径选择》，载《财经法学》2020 年第 5 期。

〔65〕 参见孔祥俊：《论反不正当竞争法的现代化》，载《比较法研究》2017 年第 3 期。

〔66〕 陈耿华：《我国竞争法竞争观的理论反思与制度调适——以屏蔽视频广告案为例》，载《现代法学》2020 年第 6 期。

〔67〕 该解释第 21 条第 2 款规定：“仅插入链接，目标跳转由用户触发的，人民法院应当综合考虑插入链接的具体方式、是否具有合理理由以及对用户利益和其他经营者利益的影响等因素，认定该行为是否违反反不正当竞争法第十二条第二款第一项的规定。”

〔68〕 参见北京知识产权法院（2016）京 73 民终 588 号民事判决书。

但真正具有决定性意义的当属消费者的自由决策利益。因为互联网不正当竞争行为对消费者利益的损害本质上体现为通过扭曲消费者的消费决策进而改变消费取向。〔69〕

三是整体意义上的公共利益受损。具体到互联网不正当竞争认定领域，其是指一种不受扭曲的互联网行业的整体竞争秩序。在个案中分析互联网领域的公共利益受损情形时，需要注意如下几个方面：（1）不应简单地将消费者利益与公共利益混同。两者虽有重合，但并不等同，在某些情形下可能存有明显的抵牾。（2）不应简单地将技术进步或者创新直接视作公共利益，而应以技术进步或者创新是否有利于促进与形塑良好的互联网竞争秩序，是否有助于提升社会公众可获得的总体福利作为最终依据。（3）不应片面以道德分析替代经济分析作为认定是否符合公共利益的标准。道德分析标准本身是一种模糊性的标准，〔70〕经济分析的适时引入可弥补道德分析的内在不足，确保公共利益受损认定标准的客观性。

5. 合理的竞争抗辩

此处的抗辩事由专指狭义的抗辩事由，即前述适用要件之外的影响互联网不正当竞争行为认定的有关理由。结合现有规范文本以及司法实践来看，其中可能且合理的竞争抗辩事由主要涉及“技术抗辩”。

在互联网不正当竞争司法实践领域，选择确立技术创新作为抗辩事由背后的理据考量主要在于：其一，顺应了鼓励互联网行业发展的现实需要。以网络技术作为基础支撑的互联网行业，无论是早期的诞生，还是当下的广泛普及，技术创新基本上构成了其发展的原动力。其二，契合了互联网市场竞争的内在属性与市场优先调节理念。互联网领域的市场竞争具有突出的创造性破坏属性，即奉行优胜劣汰和适者生存法则的动态竞争。〔71〕一项互联网新技术的运用，难免加剧经营者之间的竞争对抗与利益冲突，造成不同程度上的市场竞争损害，此时司法干预机制不应急于替代居于优先地位的市场调节机制，而应保持必要的审慎与克制，做到“市场的归市场”。因此，技术创新抗辩的存在，不仅能够为互联网领域合理的技术竞争预留必要的竞争空间，也可以进一步促进互联网行业的技术创新与发展。

在具体适用互联网不正当竞争类型化条款时，处理技术抗辩事由有必要把握如下内容：（1）注重技术创新的类型辨识。涉案的技术创新究竟是“真创新”还是“伪创新”？是“颠覆式创新”还是“微创新”？针对不同类型的创新，最终的抗辩事由采纳也将具有差异性。（2）强调技术创新的利益衡量，即技术创新抗辩的适用应当以提升社会总体福利作为宗旨。正如最高人民法院在“360 扣扣保镖案”中所指出的，“是否属于互联网精神鼓励的自由竞争和创新，仍然需要以是否有利于建立平等公平的竞争秩序、是否符合消费者的一般利益和社会公共利益为标准来进行判断”〔72〕。（3）重视技术创新与技术中立的区分。技术本身固然是中立的，但技术的不当使用却可以蜕变为不正当竞争的实施工具，因而技术中立并不能直接作为抗辩事由；而技术创新虽是立足于技术中立基础之上，但其进一步要求技术运用之于行业竞争、消费者利益以及公共利益的客观

〔69〕 参见谢晓尧：《在经验与制度之间：不正当竞争司法案例类型化研究》，法律出版社 2010 年版，第 17 页。

〔70〕 参见张占江：《不正当竞争行为认定范式的嬗变：从“保护竞争者”到“保护竞争”》，载《中外法学》2019 年第 1 期。

〔71〕 参见孔祥俊：《论反不正当竞争的基本范式》，载《法学家》2018 年第 1 期。

〔72〕 最高人民法院（2013）民三终字第 5 号民事判决书。

积极效果，故而可以成立相应的抗辩事由。

五、结　语

当前随着互联网经济开始步入“促进发展与规范管理相统一”的新发展阶段，通过深入推进与改进该领域尤其是新业态反不正当竞争规制，依法构建规范有序的竞争环境，防止资本无序扩张，进而营造开放、健康、安全的网络生态，已然成为完善我国社会主义市场经济体制、推动高质量发展的题中之义与内在要求。在此背景下，如何充分有效发挥作为判定网络领域竞争行为正当性的基础性条文——互联网不正当竞争类型化条款——自身所具有的规范作用，是横亘在理论界与实务界面前的一道难题。针对该规范所展开的具体研究，显然不能仅停留于法解释学维度的理论探讨，而应当重视结合法实证分析维度的现实考察。就司法实践层面而言，相关研究除了有必要全面梳理互联网不正当竞争类型化条款的适用形态以外，更为关键的在于深入剖析规则在现实运行中所面临的缺陷与弊端，诸如前述的“规范适用结构上面临‘泛化’与‘虚化’困境”“规范适用逻辑关系上呈现明显对立性”“规范适用构成要件解析上缺乏一致性”等，并最终以此为立足点寻求有针对性的改进对策，才能为互联网行业的良性有序发展提供科学合理且行之有效的规范支撑。

Abstract: The internet unfair competition typed clause conforms to the regulation demand of competitive behavior in the field of internet at the level of institutional supply. There are three judicial operation modes of internet unfair competition typed clause: independent application, dual application and ternary mixed application. In judicial practice, the existing typed clause is faced with the dilemma of “generalization” and “emptiness” in the structure of the application of norms, showing obvious opposition in the logical relationship of the application of norms, and lacking consistency in the analysis of the constituent elements of the application of norms. There are three ways to optimize the judicial application of the internet unfair competition typed clause. The first is to clarify the specific positioning of the application of different norms by clarifying the homogeneity of the application interpretation of the general clause, clarifying the direction of the application objects of the listed clauses and highlighting the distinction of the application functions of the declaration clause. The second is to adopt the “dual collaborative evaluation path” to clarify the external logical relationship between the typed clause and the general clause. The third is to build a unified application program of “pre-competitive relationship＋legal competitive interest＋specific competitive behavior＋multiple competitive damage＋reasonable competitive defense”.

Key Words: anti-unfair competition law, internet unfair competition, typed clause, general clause

（责任编辑：缪因知　赵建蕊）

财经法学 No. 6，2022
pp. 81 - 95

限制数据抓取行为的违法性认定
——以美国干扰侵权理论为视角

高建成*

内容提要：面对限制数据抓取行为的违法性认定难题，美国判例实践运用干扰侵权理论予以应对，通过行为对合同关系的损害结果征引行为的违法性。在干扰侵权理论的分析模式下，原告应就行为人对合同或预期合同关系的知悉、故意实施干扰行为、导致合同或预期合同关系中断、产生实质损害结果举证，被告需以正当理由进行抗辩，而法院以此为基础进行利益衡量。该理论及判例实践对我国司法实践具有借鉴意义：第一，可将合同及预期合同作为反不正当竞争法所保护的法益，避免在数据、产品服务上创造新的权益，实现司法审慎。第二，个案裁判中应关注客观层面的实质损害证明，并且着重考察行为人的主观意图，综合行为人对已存在的合同的认知情况、行为所涉的数据类型、双方商业模式、协商过程等证据，并结合正当性抗辩进行判断。当行为人限制他人的数据抓取旨在实现纯粹侵害他人的恶意而非为正当利益时，宜认定为不正当竞争行为。

关键词：限制数据抓取　不正当竞争　干扰侵权　合法商业目的

一、问题的提出

数字经济时代下，数据因其重要经济价值成为市场主体争相夺取的生产要素及资源。数据争夺过程亦引发诸多竞争纠纷以及裁判难题，而限制数据抓取行为的定性则是其中一项。对于不具备明显优势地位的经营者所实施的限制数据抓取行为，其法律属性的认定主要依据《反不正当竞争法》第 2 条，以及第 12 条第 2 款第 4 项。

* 高建成，南京大学法学院博士研究生。
本文为 2019 年国家社科基金一般项目“共享经济法律规制的司法路径研究”（19CFX065）的阶段性成果。

然而，受限于条款本身的高度抽象性及分析框架的模糊性，《反不正当竞争法》难以为司法裁判提供足够明确及统一的认定标准。在“字节跳动公司诉微梦创科公司不正当竞争纠纷案”中，字节跳动公司认为微梦创科公司设置 robots 协议黑名单导致其无法正常抓取数据，构成不正当竞争。一审法院围绕损害、商业道德进行论证，认为涉案限制数据抓取行为具有针对性，影响了原告产品的正常运行以及用户的使用，且与互联网行业促进信息流动的基本价值不符，因此判定构成不正当竞争。〔1〕二审法院否定一审法院对商业道德以及损害的认定，认为被诉行为应属于企业自主经营权范畴内的正当行为。〔2〕由此可以看出限制数据抓取行为中衡量双方利益冲突的复杂性。一方面，限制数据抓取是经营者自主经营之结果，而这种自主决策又是实现竞争机制的重要基础；另一方面，这种基于数据控制的排他行为也可能对竞争对手的经营活动产生干扰，甚至成为排除、限制竞争的工具，进而扰乱市场秩序。

同为限制数据抓取行为的纠纷，美国 hiQ 诉 linkedIn 案的判例经验或能提供参考。LinkedIn 是一家拥有 5 亿用户的职业社交网络服务公司，其用户在 LinkedIn 平台上发布简历和工作列表等信息，以此与其他会员建立商务联系。而 hiQ 是一家数据分析公司，其长期依靠抓取 LinkedIn 用户在 LinkedIn 平台上公开的个人资料信息进行人员分析预测产品的开发，并将产品出售给客户。2017 年 5 月，Linkedin 向 hiQ 发出通知，并采取技术手段限制 hiQ 访问和复制来自 LinkedIn 服务器的数据。hiQ 公司指控 LinkedIn 所实施的限制数据抓取行为构成对现有合同以及对预期经济关系的干扰，由此提出干扰侵权索赔。

美国反不正当竞争法并无明确定义与边界，泛指调整市场中竞争者之间关系的法律规则，其相关法律规范散见于联邦及各州制定法、判例法之中，并与知识产权法、侵权法、反托拉斯法存在交叠。〔3〕干扰侵权（the interference torts）被视作一种独立的侵权行为类型，并用于处理商业关系。美国从上百年的判例实践中发展出干扰侵权理论，并应用于限制数据抓取纠纷之中，其司法实践经验及理论积累对我国或有助益。因此，本文将以干扰侵权理论为视角，展示美国判例实践如何运用干扰侵权理论对限制数据抓取行为进行定性，总结判例经验及可行的制度智慧，为我国限制数据抓取行为的违法性认定提供参考。

二、干扰侵权理论的功能与违法性征引

对于数字经济时代下的竞争，行业内通常未形成长期稳定的商业惯例，因而司法机关有时难以通过行业秩序与商业道德判断竞争行为的违法性。此时可以通过国内外既有理论的挖掘与阐释，寻找行为定性的可能路径。而干扰侵权理论则是其中一种可能，其将合同关系视作财产利益，要求他人予以一定程度的注意与尊重，当行为人故意干扰时，比如明知他人存在合同关系而以技术手段限制他人抓取数据以影响交易，则可能征引其违法性。

〔1〕 参见北京知识产权法院（2017）京 73 民初 2020 号民事判决书。

〔2〕 参见北京市高级人民法院（2021）京民终 281 号民事判决书。

〔3〕 参见〔德〕博德维希：《全球反不正当竞争法指引》，黄武双等译，法律出版社 2015 年版，第 768－769 页。

（一）干扰侵权理论的起源与发展

干扰侵权理论认为，没有正当理由干涉他人与第三方之间经济关系的任何人，应当承担赔偿责任，其中经济关系既包括合同关系，也包括预期合同。干扰侵权理论具有深厚的历史渊源，最早可追溯至罗马法时期，〔4〕但其最直接的近代渊源应是19世纪中期的英国普通法实践，即1853年英国的Lumley诉Gye诱导违约案。〔5〕该案中，歌剧歌手Wagner与原告约定在原告剧院进行一定期限的演唱，并且在该期限内不得在其他地方演唱。而被告Gye在知悉两人合同的情况下，以更高费用诱导Wagenr违约并与自己缔约。〔6〕在该案中，王座法庭（Queen's Bench）认为，满足以下要件则可构成侵权：（1）被告的行为出于恶意；（2）原告与被诱使违约人之间存在有效且具有约束力的合同；（3）本合同为在特定期限内提供独家个人服务的合同。〔7〕该规则被称为“Lumley规则”，为后来的干涉合同案例所广泛采用。〔8〕随着长期判例实践的经验积累，干扰侵权理论不断得到发展，适用范畴拓宽至几乎所有类型的合同，甚至可以适用于预期合同关系。由此，该理论在发展过程中形成了干扰合同与干扰预期合同两种责任认定路径。

在美国多个司法辖区内，干扰合同以及干扰预期合同均构成侵权行为。对于干扰合同行为，《美国侵权法第二次重述》第766条规定，故意、不当干扰他人与第三人履行合同（婚姻合同除外），引诱或者以其他方式致使第三人不履行合同的，应当对第三人不履行合同给对方造成的经济损失承担赔偿责任。〔9〕而对于干扰预期合同行为，《美国侵权法第二次重述》第766B条规定了故意干扰预期合同关系行为，这是指一方故意和不正当干涉另一方未来的合同关系（婚姻关系除外），包括诱导或以其他方式导致第三人未建立或继续未来的关系，或阻止对方获得或继续未来的关系。〔10〕这两类干扰侵权规则，旨在保护原告的合同履行利益及合同不受第三人侵犯的利益，将这种合同所代表的承诺利益上升为一种财产利益进行保护。〔11〕而在部分司法辖区比如加利福尼亚州，干扰侵权通常与不公平竞争法具有交叠关系，即当行为被认定构成干扰侵权时，同时也将获得不公平竞争行为的违法性评价。

（二）理论的价值功能：维护市场竞争与交易秩序

干扰侵权理论的功能与价值目标在于维护稳定的交易秩序。干扰侵权理论起初的价值理念在于保护合同稳定性。合同稳定性具有重要的社会意义，体现为两方面：一是社会中大量不特定原告期望其所享有的承诺利益能够实现，这不限于个别原告的经济预期，更在于对承诺利益的保护有助于创造并确保额外的财产价值，从而进一步促进社会福利；二是合同稳定性有助于商业领域

〔4〕 See Francis Bowes Sayre, Inducing Breach of Contract, 36 *Harvard Law Review* 663, 663 (1923).

〔5〕 See Harvard Law Review Association, Tortious Interference with Contractual Relations in the Nineteenth Century: The Transformation of Property, Contract, and Tort, 93 *Harvard Law Review* 1510, 1522 (1980).

〔6〕 See Lumley v. Gye (1853) 2 El. & Bl. 216. 118 Eng. Rep. 749 (Q. B. 1853).

〔7〕 参见前引〔4〕，Francis Bowes Sayre文，第669页。

〔8〕 See Harvey S. Perlman, Interference with Contract and Other Economic Expectancies: A Clash of Tort and Contract Doctrine, 49 *University of Chicago Law Review* 61, 64 (1982).

〔9〕 See Restatement 2d of Torts § 766 (1979).

〔10〕 该行为在美国各州存在不同称呼，比如预期经济优势、预期经济利益，但含义均指向未订立的合同。See Restatement 2d of Torts § 766B (1979).

〔11〕 参见前引〔5〕，Harvard Law Review Association文，第1529页.

的秩序构建以及价值实现，并能有效降低社会成本。稳定的合同关系是市场经济的重要基础，市场参与者基于合同关系可以规划未来商业活动、优化经营以及协调与其他交易相对人的关系。〔12〕而随着对自由竞争价值的重视，干扰侵权理论逐渐分化为干扰合同理论以及干扰预期经济关系理论，以承担不同的功能，前者实现民事主体之间（包括经营者之间）交易安全的保障，后者调整竞争秩序，避免对竞争的不当干预。但两者在维护健康稳定的市场交易秩序的目标上体现出共同的取向。

美国将干扰侵权理论作为一项商事侵权规则来调整市场竞争者之间的关系，与我国反不正当竞争法的目的与效果具有同一性。〔13〕换言之，美国的商事侵权规则实际上以衡平法的方式发挥着规制不正当竞争行为的作用，而从目的来看，美国商事侵权规则与我国反不正当竞争法具有共同的价值追求，即识别并遏制市场内的不正当竞争行为，避免竞争者之间降低底线展开“逐底竞争”，从而维护健康良好的市场秩序。既然限制数据抓取行为存在扰乱市场秩序之可能，就需要借助法律制度以及理论工具来解决限制数据抓取行为的法律定性问题，进而维护市场竞争秩序。

（三）干扰侵权理论下限制数据抓取行为的违法性征引

经营者基于自身的商业利益以及数据安全的考量而对自身数据采取措施，限制他人抓取，体现出防御性以及被动性。这种行为本身属于自主决策范畴，不能够当然征引违法性。加之限制数据抓取手段本身难言违背商业道德以及社会认知，因而反不正当竞争法及相关法律并不会直接将其类型化为一种违法行为。

限制数据抓取行为是否会导致一方竞争优势的削弱，已有的案例给予了回答。随着数据要素的商业价值显现，掌握数据或者数据外泄均引发市场内不同经营者竞争优势的变化。数据如未得到保护与有效控制，对于控制数据一方的经营者而言可能意味着运营、财产安全受影响，经济利益遭损以及相关法律施加的义务无法实现。但对于需求数据而实施抓取行为一方而言，其由于前者的限制行为而无法获得数据，可能将难以继续其商业模式，同样存在损失经济利益的可能。

因此，在无法直接征引行为违法性的情形之下，通过干扰侵权理论对限制数据抓取行为进行评判是可行之举。首先，干扰侵权行为是一种侵权行为，因对他人合法权益具有侵害性而被赋予法律上的负面评价。也正是由于行为的侵害性，美国部分州将其视作一种不公平竞争行为。比如在加利福尼亚州，任何非法、不公平或欺诈性商业活动或行为均属于不公平竞争法所禁止的行为，而干扰侵权则属于其中的非法行为。其次，干扰侵权理论以合同所代表的承诺利益以及经济利益的归属为侵害内容，将合同视作财产利益进行保护，因而这种利益也获得要求他人不得侵害以及可寻求救济的排他功能。通常而言，无损害则无救济。在干扰侵权理论中，经济利益受到第三人侵犯是寻求救济的基础，由此引发对行为违法性的认定问题。而限制数据抓取行为本身非法律所禁止的类型化行为，其既可能是经营者自主经营的外在表现，也可能成为经营者故意破坏他人合同关系的手段及工具。而当他人合同关系或者利益归属受到侵犯时，则可以该损害结果为始点，考察限制数据抓取行为与损害结果之间的因果关系，并结合经营者的主观状态与客观证据进

〔12〕 See John Danforth, Tortious Interference with Contract: a Restatement of Society's Interest in Commercial Stability and Contractual Integrity, 81 *Columbia Law Review* 1491, 1515 (1981).

〔13〕 参见李扬、蓝小燕：《竞争法视点下的引诱违约行为研究》，载《私法》2020 年第 2 期。

行违法性分析。当限制数据抓取并非旨在促进自身经济利益或合法利益，而是为实现破坏他人经营、削弱他人竞争优势之目的时，则行为具备道德及法律上的可谴责性，由此征引行为的违法性。

三、干扰侵权的构成要件与分析模式

关于干扰侵权的构成，美国不同司法辖区对证明对象的要求不完全一致，一般包括对合同或预期合同关系的知悉、干扰行为、主观状态、损害结果。以加利福尼亚州为例，原告需就干扰合同的诉因证明以下要件：第一，原告与第三方之间存在有效的合同；第二，被告知悉该合同；第三，被告故意实施诱导违反或干扰合同关系的行为；第四，合同关系的实际违反或中断；第五，导致损害。〔14〕而针对干扰预期合同行为的证明要求与其类似，但原告还需要证明干扰手段本身违反既有相关法律规范，即具备独立的不法性。〔15〕

（一）干扰侵权的证明对象

具体而言，干扰侵权的证明对象包括：第一，原告具有合法有效的合同或者潜在的商业关系，这类关系所衍生的合同利益与预期合同利益是干扰侵权理论所保护的对象。原告应当证明合同关系是合法且存续的，比如数据分析公司开发特定数据产品服务并出售，则其与客户公司之间的买卖合同可获得保护，进而排除他人恶意干扰。如果受干扰的合同违法或者违反公共政策，则不受法律保护。比如，合同系垄断协议或侵犯他人商业秘密，则因违反法律、公共政策而无法构成干扰侵权理论的保护基础。〔16〕

第二，干扰侵权要求行为人的主观状态是故意，即行为人的主要意图在于促进干扰结果的发生。因而原告需要证明行为人知悉合同的存在，以及行为人在知悉合同以及干扰后果的前提下仍然故意干扰合同的履行。确定行为人意图与动机对于认定干扰行为是否非法具有重要意义。如果干扰是行为人的唯一或主要目的，则几乎可据此认定干扰行为不正当。因为对社会而言，纯粹侵害他人的行为与动机毫无助益，甚至可能有碍于社会的发展。然而，在干扰并非行为人所期望而纯属偶然而导致的情形之下，则需要结合干扰手段对行为进行评判。〔17〕美国部分司法辖区的判例实践也存在要求原告证明行为人存在“恶意”的做法，认为主观上的恶意是承担责任的必要条件。从其裁判过程来看，行为人的恶意通常等同于行为“缺乏正当性”。〔18〕

第三，被告实施了干扰行为，且该干扰行为导致了损害结果。原告需要证明行为、损害结果以及两者之间的因果关系。首先，此处所要求的行为要件是指行为人客观上实施了行为本身，暂不涉及行为本身的价值评判。其次，对于损害结果要件，可以表现为现有合同关系的中断以及交易机会的丧失等，分别对应干扰合同行为以及干扰预期合同行为。而企业退出市场也可满足损害

〔14〕 See hiQ Labs, Inc. v. LinkedIn Corporation, 938 F. 3d 985, 996 (2019).

〔15〕 See Facebook, Inc. v. BrandTotal Ltd., 499 F. Supp. 3d 720, 742 (2020).

〔16〕 See Restatement 2d of Torts § 774 (1979).

〔17〕 See Restatement 2d of Torts § 767 (1979).

〔18〕 See Nitzberg v. Zalesky, 370 So. 2d 389, 391 (1979); Monarch Indus. Towel and Uniform Rental, Inc. v. Model Coverall Service, Inc., 178 Ind. App. 235, 236 (1978).

结果要件，并在程度上更为严重。此外，因果关系亦是不可缺失的一环，原告需证明损害结果是由被告行为直接导致，将责任主体明确指向行为人。

第四，干扰手段非法性的证明问题。一般而言，对于干扰合同的主张，原告无需证明干扰行为的手段具有非法性，而对行为要件的证明止步于事实层面。但手段上的独立非法性证明对于干扰预期合同行为而言通常是必要的。独立不法性意味着手段本身构成独立的侵权行为或违反现有的宪法、刑法、反托拉斯法等法律，其将直接影响法院的利益衡量结论。如果干扰手段本身包含侵权行为，例如诽谤、致害诋毁、欺诈、暴力或威胁，那么无论是干预合同还是预期合同，行为均无正当性可言；干扰方式构成限制贸易的共谋或行动等反托拉斯行为，或者，根据辖区内的法律构成违法，如干扰手段构成加利福尼亚州不公平竞争法所禁止的任何非法、不公平或欺诈性的商业行为，同样满足独立不法性的要求。〔19〕

（二）干扰侵权的正当性抗辩及利益衡量

在市场经济之下，自由竞争所带来的损害具有相对性与必然性，合理的竞争行为不应得到法律的否定性评价，否则将威慑市场竞争，并且提高交易成本。〔20〕因而，在程序上赋予被告抗辩的机会有助于法院的综合考虑，避免错误干涉竞争。面对原告的干扰侵权主张，被告可以就其行为的正当性进行积极抗辩，证明自身行为以及所追求利益的合理性。比如证明自身行为是为了实现合法的商业目的而非基于破坏其他经营者的竞争优势之目的；又如干涉合同是基于传染病防控，保护健康、安全或者良好道德的目的；〔21〕再如，合同的执行不利于劳动者合法权利保障〔22〕。若抗辩成立，被告没有采取不正当或违法手段进行干扰，则无需承担侵权责任。

而对于干扰预期合同而言，被告享有更为广泛的正当抗辩事由，可以主张竞争特权抗辩。换言之，如果原告没有成功订立合同，则被告可以在没有采取非法手段的前提之下，以正当竞争为由从原告处争取交易机会。其中主要的考虑在于，第一，预期合同作为一种预期的、潜在的利益，与已缔约的合同利益所代表的稳定期待有所不同，其保护力度应弱于合同。第二，对干扰预期合同的认定标准过低，将严重打击市场竞争，损害市场预期并增加市场交易成本，进而违背市场经济的初衷。竞争通常被认为能够有效地进行资源分配，并以最低成本维护谈判环境。〔23〕“在以自由竞争原则为基础的经济体制中，竞争者不应因寻求合法商业优势而承担侵权责任。”〔24〕而要求原告证明行为不法性的规则，有助于减少经营者的诉讼风险，降低无合同环境下的竞争成本与交易成本。〔25〕

随后，在被告对干涉合同的正当理由举证后，由法院进行利益衡量。关于干扰侵权理论中的

---

〔19〕 See Cal. Bus. & Prof. Code § 17200.

〔20〕 See Gary Myers, The Differing Treatment of Efficiency and Competition in Antitrust and Tortious Interference Law, 77 *Minnesota Law Review* 1097, 1140－1141 (1992).

〔21〕 See Harvard Law Review Association, Inducing Breach of Contract-Justification-Effect of Motive, 38 *Harvard Law Review* 115, 115－116 (1924).

〔22〕 See Hitchman Coal and Coke Co. v. Mitchell, 38 S. Ct. 65 (1917).

〔23〕 参见前引〔8〕，Harvey S. Perlman 文，第 83－84 页。

〔24〕 前引〔20〕，Gary Myers 文，第 1122 页。

〔25〕 See Jesse Max Creed, Integrating Preliminary Agreements into the Interference Torts, 110 *Columbia Law Review* 1253, 1267－1268 (2010).

价值位阶，一般认为，公共利益优先于私人利益，生命健康利益优先于财产利益。法院的利益衡量将以合同的稳定性所代表的利益作为判断基准，进而根据价值位阶进行衡量，判断干涉行为所保护的利益是否超过合同的稳定性所代表的利益。〔26〕在已有合同的情形下，合同利益的位阶优先于竞争自由利益，被告如果以竞争特权作为抗辩事由，则无法得到支持。

四、干扰侵权理论下限制数据抓取行为的判例实践

干扰侵权理论为认定限制数据抓取行为的法律属性及行为人的责任提供了初步思路与分析框架，强调了对干扰意图的考证。如果干扰旨在改善自身业务等合法目的，而非破坏他人商业关系，通常不被认为违背商业道德或违反侵权法。并且，干扰侵权制度与禁令救济常常密不可分。作为干扰侵权的重要救济方式，禁令的申请在损害严重程度、利益衡量方面有更严要求。从干扰侵权制度的构造来看，法院谨慎地介入竞争关系的规制。但这并不影响经营者以该制度作为商业竞争中的维权武器。在认识该制度的基本构造之后，可通过限制数据抓取纠纷的判例实践考察理论的具体应用。

（一）hiQ 诉 LinkedIn 案

在 hiQ 诉 LinkedIn 案中，hiQ 指控 LinkedIn 限制数据抓取的行为构成干扰侵权并申请临时禁令。第九巡回法院在利益衡量的过程中，充分考虑 LinkedIn 的动机以及手段正当性问题，进而支持了 hiQ 的干扰侵权索赔，并保护了 hiQ 公司与其客户之间的合同关系。

该案中 hiQ 提出干扰侵权索赔并充分证明了干扰侵权行为的要件，即行为人在清楚认识到他人存在商业关系的情况下仍然实施干扰。首先，LinkedIn 知悉 hiQ 的商业模式以及其可能存在的商业关系，因 LinkedIn 曾派代表参加 hiQ 展现商业模式与产品的会议以及商演现场，清楚认识到 hiQ 依靠 LinkedIn 的公开数据进行分析研发的情况。其次，LinkedIn 以法律责任威胁 hiQ，并实际采取技术措施以限制 hiQ 对数据的访问，由此满足干扰侵权的故意实施行为的要件。再次，hiQ 与第三方之间的合同关系已经中断，因其无法访问 LinkedIn 的数据而无法按照承诺向现有客户提供服务。最后，hiQ 因现有合同中断和对预期合同的干扰而受到损害，即丧失产品销售收入，而且很可能导致倒闭。〔27〕

LinkedIn 则以合法的商业目的进行抗辩，认为限制数据抓取行为是为了保护用户隐私以及自己的投资利益。第九巡回法院认为，第一，LinkedIn 阻止 hiQ 访问 LinkedIn 服务器上的数据的行为不是一种公认的正当贸易行为。一方面，从 LinkedIn 的行为表现来看，涉案数据本是公开数据，而 LinkedIn 阻止 hiQ 访问、抓取数据具有针对性以及选择性，不符合广告、降价等公认的商业惯例。另一方面，从 LinkedIn 的行为结果来看，其限制行为将根本地、直接地破坏竞争对手的基本商业模式。第二，法院认为，LinkedIn 仅针对作为潜在竞争对手的 hiQ 实施限制，很可能是为了促进 LinkedIn 自身在数据分析工具领域的竞争优势，并将竞争对手逐出数据分析市

〔26〕 See Imperial Ice Co. v. Rossier，18 Cal. 2d 33，36 (1941).

〔27〕 See hiQ Labs，Inc. v. LinkedIn Corporation，938 F. 3d 985，996 (2019).

场，因此该行为可能不在“公平竞争范围内”，很可能违反加利福尼亚州不公平竞争法而构成违法垄断。[28]

（二）Facebook 诉 BrandTotal 案

在另一起限制数据抓取纠纷中，法院起初没有支持干扰侵权索赔。2020 年 9 月，Facebook 公司关闭 BrandTotal 公司在 Facebook 有关网站的账户，并采取技术措施，阻止 BrandTotal 对 Facebook 数据的访问与抓取。10 月，Facebook 向加利福尼亚州法院起诉 BrandTotal，而 BrandTotal 则提起反诉，认为 Facebook 的限制数据抓取行为构成干扰侵权以及不公平竞争，导致其与客户的合同破裂，并申请临时限制令。[29]

在干扰侵权索赔的辩驳中，Facebook 声称限制数据抓取是为了实现合法的商业利益，即通过阻止 BrandTotal 的访问遵守法律施予的义务，因而申请驳回 BrandTotal 的反诉。而其中的法律义务，源自美国联邦贸易委员会（FTC）的执法行动命令，FTC 要求 Facebook 采取措施以防止第三方违反隐私设置以及用户条款进行数据抓取。[30] 双方均不质疑遵守法律要求可以作为干扰侵权的抗辩理由。此外，法院基于 BrandTotal 的行为表现，倾向于认可 Facebook 公司的合法商业理由：一方面，Facebook 本身已建立了共享数据的渠道，比如 API 方式，而 BrandTotal 没有事先与 Facebook 就获取数据的有关事项进行沟通，因而难以判断 Facebook 的意图；另一方面，Facebook 认为 BrandTotal 有以不当方式收集用户数据的历史，有可能威胁用户隐私安全。[31] 因此，BrandTotal 在初次提出的反诉中未能成功证明干扰侵权，其主张未得到法院认可。

由于干扰手段的合法性问题同样会影响法院的利益衡量结果，BrandTotal 起初试图通过援引 hiQ 案以证明 Facebook 行为构成垄断。BrandToatl 认为 Facebook 限制抓取的数据包括公开数据，其情形与 hiQ 案相同，均违反加利福尼亚州不公平竞争法并构成垄断。而法院根据 Facebook 限制抓取的不同数据展开类型化讨论：第一，针对公开数据，比如 Facebook 为用户生成的广告偏好以及特定广告参与度的有关分析数据，通常不涉及知识产权以及用户隐私，而 Facebook 限制此类数据的抓取，则可能存在与 hiQ 案中类似的垄断公共信息之风险，可能构成不公平竞争行为或者非法垄断。[32] 但法院补充道，具体还需要结合 BrandTotal 与 Facebook 的协商过程等证据对 Facebook 的真实动机进行考察。第二，针对非公开数据，这类数据通常受密码保护，且承载用户隐私内容，因此 Facebook 对此进行保护与监管是合理且合法的。Facebook 上的用户可以选择与特定对象共享信息，且基于 Facebook 的隐私设置以及用户条款而存在合理的隐私期待，以免受于第三方的数据抓取。[33] 因此，Facebook 存在执行自身合同方面的利益，这种利益同样受法律保护。在此情况下，法院认为判断 Facebook 是否担责的关键就在于行为是否

〔28〕 See hiQ Labs，Inc. v. LinkedIn Corporation，938 F. 3d 985，998 (2019).
〔29〕 See Facebook，Inc. v. BrandTotal Ltd.，499 F. Supp. 3d 720 (2020).
〔30〕 See Facebook，Inc. v. BrandTotal Ltd.，499 F. Supp. 3d 720，739 (2020).
〔31〕 See Facebook，Inc. v. BrandTotal Ltd.，499 F. Supp. 3d 720，742 (2020).
〔32〕 See Facebook，Inc. v. BrandTotal Ltd.，499 F. Supp. 3d 720，739 (2020).
〔33〕 See Facebook，Inc. v. BrandTotal Ltd.，499 F. Supp. 3d 720，740 (2020).

出于善意。[34] 但由于 BrandTotal 在干扰侵权问题上没能证明 Facebook 的恶意，法院经利益衡量后更倾向于支持 Facebook 的正当理由抗辩，认为 Facebook 在监管平台整体的安全方面存在较强的商业利益。鉴于 BrandTotal 就案件的实质问题提出了严重质疑，法院允许 BrandTotal 后续修正干扰侵权、不公平竞争等相关反诉。

在 2021 年 6 月，BrandTotal 经再次修正反诉后，成功证明 Facebook 的干扰恶意，致使其干扰侵权索赔得到法院支持。转折点在于，BrandTotal 声称并举证 Facebook 以欺诈以及误导性陈述的手段促使 Google 从其应用商店中下架 BrandTotal 的产品。Facebook 曾于 2019 年对 BrandTotal 的产品进行调查，调查结果表明其产品无害。Facebook 在当时并未采取任何行动，直到 2020 年，在 Facebook 收到广告客户对 BrandTotal 能力的询问后几天，随即要求 Google 对 BrandTotal 进行处理。BrandTotal 举证，Facebook 在与 Google 交涉时未如实披露相关信息，并虚构 BrandTotal 的不当行为。而 Facebook 未能对该恶意证据进行解释，因而其合法商业目的抗辩最终被驳回。[35]

五、基于限制数据抓取纠纷裁判的因素归纳

在自由竞争的市场经济背景下，竞争行为表现出复杂的利益冲突以及交易机会的此消彼长，仅具有干扰外观并不当然意味着具有不正当性。纯粹破坏他人经济关系的恶意行为才需要给予负面法律评价，而干扰侵权理论之适用则有助于对其形成约束。干扰侵权的构成要件以及举证责任分配难度不大，难点在于对具体要件的进一步考量以及利益衡量过程的把握。从前述判例实践的焦点来看，欲以干扰侵权理论认定行为违法，应着重考虑干扰行为所致的损害、干扰行为人的主观状态以及正当理由抗辩。这些因素的考虑都旨在辨识干扰人的主观目的是否为损害、破坏他人的经济关系。

（一）实际损害之程度

对于限制数据抓取行为而言，禁令救济是较为重要的救济方式。在衡平法上以干扰侵权为诉因申请禁令，无论是申请临时禁令还是永久禁令，都应当以实质损害的发生为基础，并且应满足特定程度的要求，即造成无法弥补的损害。无法弥补的损害不能仅是单纯的金钱损失，从限制数据抓取的判例实践来看，法院所认可的无法弥补的损害包括大部分业务的中断、潜在客户或商业损失、退出市场的风险等，需要通过原告对损害的举证予以支撑与说明。比如 hiQ 诉 LinkedIn 案中 hiQ 声称的可能面临的倒闭风险，[36] 以及 Facebook 诉 BrandTotal 案中 BrandTodtal 所举证的潜在商业客户以及商誉的损失等无形损害[37]。

一般而言，市场竞争下交易机会的流失是经营者所面临的正常现象，因而无形损害若要寻求

〔34〕 See Facebook, Inc. v. BrandTotal Ltd., 2021 WL 662168, 8-9 (2021).
〔35〕 See Facebook, Inc. v. BrandTotal Ltd., 2021 WL 2354751, 8-9 (2021).
〔36〕 See hiQ Labs, Inc. v. LinkedIn Corporation, 938 F. 3d 985, 993 (2019).
〔37〕 See Facebook, Inc. v. BrandTotal Ltd., 499 F. Supp. 3d 720, 736 (2020).

救济需要达到足够的程度。〔38〕正如 BrandTotal 指出，其已无法获取为维持运营所必要的数据，被迫暂停大部分业务。同时，BrandTotal 通过特定客户对 Facebook 指控的担忧、特定潜在客户暂停或推迟与 BrandTotal 的谈判，以及风险投资损失等内容的举证，确认了其所遭受损失达到了无法弥补的程度。

（二）主观动机之考虑因素

识别行为人的主观动机通常依赖于客观行为证据，由此应关注客观行为的外在表现。当行为具有非法性时，比如诱使他人限制数据抓取或限制产品的功能是通过诽谤、致害诋毁、欺诈等手段作出，则可以基本确定行为人的恶意。如果未能直接识别非法性，则应该充分考察限制数据抓取的外在行为表现，包括行为人对已存在合同等经济关系的了解情况、行为相关的数据类型、协商过程、竞争关系等因素。

第一，行为人对已存在合同关系的认知。如干扰人并不存在知悉他人存在合同关系之可能，则其行为难言是旨在破坏他人经济关系。需注意的是，对已存在的合同的认知情况并不需要特别细致，无需证明干扰人知道合同相对人是谁以及具体合同内容，只要证明干扰人知道自己在干扰他人合同即可。〔39〕

第二，数据类型有助于考察行为主观意图，但并非决定因素。hiQ 案以及 Facebook 案一致认为，对于非公开数据而言，经营者基于自身商业模式，通过密码保护、技术手段、用户协议、隐私设置等方式对数据进行保护，体现出强烈的保护需求以及维持经营的动机，因此限制数据抓取难以体现侵害的恶意。而对于公开数据的限制抓取，可能违反加利福尼亚州不公平竞争法以及反托拉斯法，进而在手段上显现出违法性。原被告双方是否为竞争关系亦有助于考量被告行为的动机。如 hiQ 案中，LinkedIn 与 hiQ 在数据分析产品市场上具有竞争关系，且 LinkedIn 具备可观的数据资源与市场地位优势，在无正当理由的前提之下以限制访问的手段干扰 hiQ，很可能构成干扰侵权以及垄断。美国第九巡回上诉法院论述道："如果像 LinkedIn 这样（拥有大量公共数据）的公司被允许有选择性地禁止潜在竞争对手访问和使用公共数据，将导致收集和分析公共数据领域的原始创新者被排除于市场之外。"〔40〕但具体定性仍需作进一步的分析，即针对公开数据的限制抓取亦并不当然非法，比如 Facebook 案中，法院认为 Facebook 有可能存在急需实现的重要利益，或者基于平台数据的整体监管而无法实现对某类数据的独立操作，这些情况均可能证明行为人的动机并非损害其他经营者。因而，数据类型是其中一项考量因素，但并不能简单地基于数据的公开状态而断定限制抓取违法。BrandTotal 曾三次修改有关 Facebook 涉嫌垄断的不公平竞争反诉主张，均未成功证明。

第三，限制数据抓取行为的主观意图还可以结合双方的协商洽谈记录进行判断。合同是处理数据权益、配置的一种重要方式，数据交易应当尊重市场原则以及双意愿，避免削弱市场竞争的激励机制。出于对数据处理者的劳动成果以及相关财产利益的尊重，抓取数据一方应当积极寻求

〔38〕 See Rent-A-Center, Inc. v. Canyon Television and Appliance Rental, Inc., 944 F. 2d 597, 603 (1991).

〔39〕 See Facebook, Inc. v. BrandTotal Ltd., 499 F. Supp. 3d 720, 738 (2020).

〔40〕 hiQ Labs, Inc. v. LinkedIn Corporation, 938 F. 3d 985, 998 (2019).

同意。通过寻求协商与同意，需求方或能以较小成本实现数据获取的目的，并避免违法风险。而对于司法裁判来说，协商过程能够帮助法院比较不同合同或者合作方式，从而考察行为人是否设置不合理的交易条件，以及是否具备排除限制竞争的动机与目的。比如美国北卡罗来纳州法院指出："鉴于 Facebook 拒绝 BrandTotal 的访问，是基于 BrandTotal 未能与 Facebook 协商并通过 Facebook 的现有渠道（比如 API）以寻求许可……任何一方都未能就 BrandTotal 如何获得 Facebook 的许可问题进行协商，因而留下了一个悬而未决的问题，即 Facebook 的意图，以及如果 BrandTotal 在符合 Facebook 授权访问协议范围内开展业务，Facebook 是否会同意许可。"〔41〕在数据控制者已经存在共享数据的途径、渠道及方式的情形之下，如果抓取数据一方没有积极寻求协商，或者没有遵守明确权利义务的用户协议进行数据抓取，则不宜直接推定限制抓取一方的动机。

当限制数据抓取行为是通过第三人实现时，如行为人通过虚假陈述等手段导致第三人采取措施干扰合同履行，则法院还应考察行为人与第三人的协商过程。在 Facebook 案中，Facebook 除了自行采取技术措施限制 BrandTotal 的抓取行为外，还通过虚假陈述误导 Google 应用商店下架 BrandTotal 的产品，该行为是法院认定其干扰恶意的关键。因而，类似案件的裁判也应当将沟通内容的客观性、中立性纳入主观恶意的考察范围。

（三）合理商业目的与利益衡量

由被告就限制数据抓取的合理商业目的进行阐释与举证，是合理的制度安排，有助于法院考察真实的行为动机、更好地进行利益衡量。一般认为，行为人没有正当理由而损害其他经营者的利益，可以认定其具有纯粹损害他人的恶意，进而应当承担法律责任。在市场竞争之中，合理的商业目的具有丰富的表现形式与内涵，立法无法完全穷尽。就限制数据抓取纠纷的判例实践来看，限制数据抓取的正当理由抗辩通常包括私人利益保护与公共利益保护两方面。私人利益保护的需求可表现为保护投资安全、保护平台监管的完整性、以自力救济防御第三方侵害等；而与公共利益相关的限制数据抓取的商业目的与正当利益，主要是遵守法律要求，比如保护用户隐私可以作为豁免责任的理由。

在考察正当理由抗辩时，应当探析正当理由与行为之间的因果关系，正如 hiQ 诉 LinkedIn 中，LinkedIn 以隐私保护为由进行抗辩，第九巡回上诉法院在进行利益衡量时指出：一方面，LinkedIn 的核心商业模式是为用户提供信息共享的平台，并不需要禁止 hiQ 访问数据来实现开发平台的投资保护目的；另一方面，用户对其公开档案中共享的信息所寄予的隐私期望是不确定的，并且 LinkedIn 自身也开发了一项与 hiQ 产品类似的数据分析产品，因而其所声称的隐私保护目的很可能是借口。〔42〕

在利益衡量环节，限制数据抓取行为经常涉及双方兼具合法权益的情形，因而需要确定价值位阶。当双方利益处于同一位阶时，比如双方均有迫切实现的合同利益，则要求证明行为人特定的动机。比如前述 Facebook 案中，Facebook 认为自己的行为存在正当利益，即执行用户协议，而该利益同样受法律保护。在此情况下，"决定性问题就在于被指控干涉一方是否出于

〔41〕 Facebook，Inc. v. BrandTotal Ltd.，499 F. Supp. 3d 720，742（2020）.

〔42〕 See hiQ Labs，Inc. v. LinkedIn Corporation，938 F. 3d 985，998（2019）.

善意行事”〔43〕，如不能证明其恶意，则难以施加责任。BrandTotal 曾因并未证明 Facebook 的特定动机或恶意导致其基于干扰合同提起的反诉被驳回，法院认为：“BrandTotal 承认 Facebook 的服务条款，其禁止未经许可自动收集数据的行为。尽管 BrandTotal 在其关于当前驳回动议和之前的临时限制令动议的诉状中暗示 Facebook 存在恶意，但 BrandTotal 并未在其反诉中指控 Facebook 存在任何特定动机。”〔44〕

六、启示与总结

通过美国判例实践的展示，可以洞见美国司法的审慎态度，其对干扰侵权理论的适用更为精细，并通过损害程度要求、正当性抗辩环节及主观恶意证明等提高认定行为违法性的门槛，体现了司法机构对市场竞争的尊重，避免过度干预。也由于利益衡量环节的加入，反不正当竞争法的适用不至于将一方的商业利益上升为“绝对权利”，进而加以偏颇保护，导致静态竞争利益的固化。干扰侵权理论与实践对于认定限制数据抓取行为的违法性具有一定助益，为司法机关提供了利益衡量与价值评判的基本范式。尽管中美两国具有不同的法系背景与传统，但该理论以及相关实践具有一定的借鉴价值。

（一）我国侵害债权理论及相关立法基础

我国学界早已对干扰侵权理论进行探讨，且存在一定的立法基础。基于法系背景差异，合同履行利益在我国属于债权概念范畴，因而美国干扰侵权理论实际上与我国第三人积极侵害债权理论与法律实践具有共同性。在立法规范上，我国《民法典》为干扰侵权理论提供了法律依据。《民法典》第 1165 条作为侵权责任的一般条款，规定“行为人因过错侵害他人民事权益造成损害的，应当承担侵权责任”。而第 593 条规定：“当事人一方因第三人的原因造成违约的，应当依法向对方承担违约责任。当事人一方和第三人之间的纠纷，依照法律规定或者按照约定处理。”合同作为一项债权属于民事权益范畴，而当第三人因过错对合同权益实施侵害且造成损害结果时，债权人基于侵权事实向第三人主张侵权责任并不与立法规范相悖。针对这种行为的调整，学界有大量观点主张可以以侵权法解决当事人与第三人的纠纷。〔45〕基于市场交易的经验与习惯，社会观念层面已普遍承认对合同归属与履行利益的保护与尊重。尽管合同作为债权不具备典型的社会公开性，但一旦行为人知悉债权关系的存在即满足了具体公开性之要求。行为人在感知他人权益状况的前提下实施侵害，存在过错以及可责性，由此征引行为的违法性，进而追究行为人的侵权责任并实现对受害人的救济。〔46〕

而将视野扩展至市场竞争领域，第三人侵害债权理论或干扰侵权理论即是对诚实信用原则的

〔43〕 Facebook，Inc. v. BrandTotal Ltd.，2021WL662168（2021）；Richardson v. La Rancherita，98 Cal. App. 3d 73，81（1979）.

〔44〕 Facebook，Inc. v. BrandTotal Ltd.，2021WL662168，8（2021）.

〔45〕 参见王利明：《违约责任论》，中国政法大学出版社 2003 年版，第 743 页；解亘：《论〈合同法〉第 121 条的存废》，载《清华法学》2012 年第 5 期；施鸿鹏：《债权的侵权法保护及其法理构成》，载《法学家》2022 年第 1 期；程啸：《侵权责任法》，法律出版社 2021 年版，第 178 页。

〔46〕 参见前引〔45〕，施鸿鹏文。

强调，要求市场内的经营者诚实守信，以创新与增加效率等正当途径实现竞争优势的累积，而非通过恶意干扰手段“害人利己”。这样的理念与价值目标与我国《反不正当竞争法》相吻合。由此，《反不正当竞争法》可以将干扰侵权行为视作一种违反商业道德的不正当竞争，〔47〕并通过干扰侵权理论征引限制数据抓取行为的违法性从而进行调整。抑或在分析模式层面，将干扰侵权理论与实践作为我国适用《反不正当竞争法》第 12 条（即互联网专条）的借鉴对象。两者在分析模式上并不互斥，具有一定的共通性。以《反不正当竞争法》第 12 条所列举禁止的网络不正当竞争行为作为比照，链接跳转、妨碍破坏网络产品服务的行为则可以抽象为美国干扰侵权理论中的干扰行为，在主观层面都至少应满足故意要件甚至是恶意要件，〔48〕在客观层面上则体现为网络产品或服务的正常运行受到干扰。

但两者也存在区别。干扰侵权理论所保护的权益在于合同以及预期合同，其并不以产品服务受妨碍的事实作为判断行为违法性的起点。因而，干扰侵权理论的价值可以体现为避免司法机关在产品服务、流量、数据上创造新的权益，进而控制司法干预竞争的门槛。并且，区别于“非公益必要不干扰”模式，干扰侵权模式的分析进路有助于为经营者的行为自由留存足够空间，避免对自由竞争的过分干预。“非公益必要不干扰”的分析模式源自我国法院在“百度诉奇虎案”中的裁判思路，〔49〕其预设企业之间竞争行为的非法性，并提出干扰行为只有基于公益之必要才能被认为是合法的〔50〕。而该模式对竞争行为预设非法性的先定立场以及狭隘的正当化事由，实则以绝对权保护的思维对市场先入者的竞争利益施以倾斜保护，将抑制网络市场竞争以及创新机制。〔51〕综上，美国干扰侵权理论及实践之于我国限制数据抓取行为定性乃至网络不正当竞争行为的分析框架具有借鉴意义及可能。

（二）实践应用：我国限制数据抓取行为的违法性认定

就司法实践层面的借鉴而言，作为调整市场主体竞争行为的重要法律规范，《反不正当竞争法》明确禁止多种明显扰乱竞争秩序的行为，并以第 2 条即一般条款实现兜底适用。其中，与一般条款类似，《反不正当竞争法》第 12 条第 2 款第 4 项也承担兜底适用的功能。这类兜底性规定是评价限制数据抓取行为违法性的标尺，但其为了保障法律的弹性适用效果而一定程度上牺牲了规范构造上的确定性，未能为司法裁判提供明确指引。2022 年 1 月发布的《最高人民法院关于适用〈中华人民共和国反不正当竞争法〉若干问题的解释》亦未对此进行回应，只是在第 3 条中指出法院可以参考自律公约及行业规范等认定行为是否违反商业道德。〔52〕但除了特定行业领域存

〔47〕 参见前引〔13〕，李扬，蓝小燕文。

〔48〕 参见孔祥俊：《网络恶意不兼容的法律构造与规制逻辑——基于〈反不正当竞争法〉互联网专条的展开》，载《现代法学》2021 年第 5 期。

〔49〕 参见北京市高级人民法院（2013）高民终字第 2352 号民事判决书；最高人民法院（2014）民申字第 873 号裁定书。

〔50〕 参见薛军：《质疑“非公益必要不干扰原则”》，载《电子知识产权》2015 年第 Z1 期。

〔51〕 参见宋亚辉：《网络干扰行为的竞争法规制——“非公益必要不干扰”原则的检讨与修正》，载《法商研究》2017 年第 4 期。

〔52〕《最高人民法院关于适用〈中华人民共和国反不正当竞争法〉若干问题的解释》第 3 条规定：“特定商业领域普遍遵循和认可的行为规范，人民法院可以认定为反不正当竞争法第二条规定的‘商业道德’。人民法院应当结合案件具体情况，综合考虑行业规则或者商业惯例、经营者的主观状态、交易相对人的选择意愿、对消费者权益、市场竞争秩序、社会公共利益的影响等因素，依法判断经营者是否违反商业道德。人民法院认定经营者是否违反商业道德时，可以参考行业主管部门、行业协会或者自律组织制定的从业规范、技术规范、自律公约等。”

在自律公约外，如我国《互联网搜索引擎服务自律公约》，其他领域未必存在相应的行业规范予以指引，此时无法依赖商业道德要件对行为进行价值评判，背俗侵权的分析模式也无法直接适用。并且，一般经营者限制数据抓取行为可能出于投资保护、妨害防御等正当需求，属于合法的自主经营行为，并不当然能够从限制手段中征引非法性。〔53〕因而，美国干扰侵权理论实践或有助益，能够为我国司法提供基本分析模式，并展现个案裁判中所需关注的因素，其逻辑在于，经营者恶意以限制数据手段侵害竞争对手的合同关系，导致其履行不能，行为将因侵害结果、主观恶性损害市场秩序而产生规制必要性。

从分析模式来看，美国法院从损害结果、客观行为、主观因素等方面进行利益衡量，类似于我国在制定法下结合主客观要件进行分析的模式，并通过要件下具体事实的考察，评判行为人是否应当担责。在肯定干扰侵权理论的价值之基础上，我国法院在具体裁判限制数据抓取行为纠纷中应着重关注原告两方面的举证。

在客观构成要件方面，原告需举证限制数据抓取行为所造成的实质损害结果。实际损害结果的证明是寻求救济的基础。在数据竞争行为的救济手段中，损害赔偿以及停止侵害是较为重要且主要的责任形态。而为了维持经营以及保持商业模式的可持续，原告更为期盼获得类似美国行为禁令的救济方式，以制止、预防针对未来的侵害。但由于数据具有可复制性，一旦开放则可能造成不可逆的结果，包括数据失控导致用户信息泄露、知识产权控制措施的失效、基于数据所积累的商业优势的丧失等。因而有必要对损害要件的证明施以实际损害及严重程度的要求，而不能是类似“流量减损”“消费者选择的减少”等抽象意义上的损害。需强调，并非所有由竞争机制导致的损失都具有司法救济的必要性。在竞争损害具有相对性的背景下，交易机会的此消彼长以及流量的增减是市场竞争的常态。〔54〕如果将举证门槛放宽至此类抽象损害，客观上将导致《反不正当竞争法》过于轻率地介入市场竞争中，不利于实现司法审慎。由此，应要求原告通过合同乃至商业关系的中断对实质损害及其严重程度予以证明。

在主观要件的考察方面，原告应证明行为人具备侵害合同的主观故意以及恶性意图。基于市场经济下竞争的损害必然性以及保障竞争自由最大化的考虑，应对主观要件施以故意乃至恶意的要求。而以故意作为主观要件，有助于平衡利益保护及行为自由。〔55〕至于恶意要件，首先包含希望或放任损害结果发生的故意，并强调行为人在主观意图上纯粹损害他人而非旨在实现自己的正当竞争利益，由此构成反不正当竞争法意义上的可谴责性。〔56〕在双方都具有合理的竞争利益的情形下，主观意图将成为影响违法性认定的关键所在。如果无法证明行为人的主观恶意，则不应认定限制数据抓取行为违法，否则将严重限制市场主体的经营自由。

与欺诈、胁迫、暴力等手段不同，限制数据抓取行为本身未必能直接体现非法性以及行为人的主观恶意。对于行为人恶意的考察，仍需借助客观证据进行判断。从美国 hiQ 案以及 Facebook 案的判例实践来看，应结合以下方面进行考察：第一，双方的商业模式，包括被限制

〔53〕 参见高建成：《限制数据抓取行为的正当性及其价值衡量》，载《中国流通经济》2022 年第 8 期。

〔54〕 参见前引〔51〕，宋亚辉文。

〔55〕 参见孙晋、李胜利：《竞争法原论》，法律出版社 2020 年版，第 368 页。

〔56〕 参见前引〔48〕，孔祥俊文。

方的商业活动是否以行为人的数据为必要基础，而行为人商业模式下的数据是否原本处于公开的状态；第二，双方就数据交易的协商过程，以此判别占有数据的经营者是否对其他经营者课以不公平的交易条件或者差别待遇；第三，抓取数据行为的后果，包括数据占有者的合理商业利益、法律义务要求以及抓取数据方的数据使用方式；第四，行为人是否有通过虚假陈述等方式诱使其他经营者实施限制行为；第五，行为人限制数据抓取的正当理由抗辩，应要求行为人就正当理由进行举证，以此考察合理的商业目的，判断行为意图。

由此，借鉴干扰侵权理论及实践经验，我国司法实践可从主客观层面对限制数据抓取行为进行要件式衡量与考察，进而在个案中审慎认定违法性。须明确，干扰侵权理论的目的在于规制纯粹破坏他人经营的行为，并确保其他市场主体行为自由的合理空间。如果行为旨在实现或维护正当商业利益而偶然、不可避免地导致他人的损害结果，则不宜施以法律责任；若明知损害结果的发生而无正当理由，则可体现行为人的主观恶性意图，构成不正当竞争法的可责性。

Abstract: Faced with the challenge of determining the illegality of restriction on data scraping, US jurisprudence has applied the tort of interference doctrine to address the illegality of an act by means of its detrimental effect on a contractual relationship. Under the tort of interference theory, the plaintiff shall prove that the actor had knowledge of the contractual or contemplated contractual relationship, intentionally interfered with the contractual or contemplated contractual relationship, caused the interruption of the contractual or prospective contractual relationship, and produced a materially injurious result. The theory and jurisprudence have implications for China's judicial practice. Firstly, contracts and prospective contracts can be treated as legal interests protected by the anti-unfair competition law, avoiding the creation of new rights and interests in data and product services and achieving judicial prudence. Second, case adjudication should focus on the objective level of proof of substantial damage and focus on examining the subjective intent of the actor, integrating evidence of the actor's knowledge of the pre-existing contract, the type of data involved in the act, the business model of both parties, the negotiation process, and combining with the justification defense. When the actor restricts the data capture of others with the intention of purely malicious intent to infringe on others rather than for legitimate purpose, it is appropriate to find unfair competition.

Key Words: restricting of data scraping, unfair competition, interference torts, legitimate business purpose

（责任编辑：殷秋实　赵建蕊）

财经法学 No. 6，2022
pp. 96 - 110

全球数据治理的 DEPA 路径和中国的选择

靳思远 *

内容提要：随着数字科技的发展，数据已成为各国的基础性、战略性资源。各国对数据资源的争夺日趋激烈，数据跨境流动等议题成为国际关注的焦点。由于数据兼具财产利益和人格利益属性，各国治理数据的理念存在分歧，目前数据的全球治理框架尚未形成。《数字经济伙伴关系协定》（DEPA）是全球首个针对数字经济而制定的专项协定，在数据议题上主要借鉴了美式数字规则并采用了灵活的模块式框架，反映了新加坡等中小国家在数字治理方面的诉求，相较传统综合性的贸易协定更具时代性、灵活性和可扩展性。从中国正在构建的数据出境评估体系来看，中国国内数字规则与 DEPA 等高水平国际数字规则之间存在一定的张力。中国申请加入 DEPA 有利于促进本国数字经济发展和国际合作，提升数据治理水平，进一步扩大中国在全球数据治理中的话语权。

关键词：DEPA　数字经济　全球数据治理

近年来，随着科技的迅猛发展，数据已成为全球经济活动中不可或缺的生产要素。国家通过制定数字规则、缔结和参加国际协定等方式参与全球数字经济治理，力求在全球数字经济竞争中获得优势。2020 年中国数字经济规模为 5.4 万亿美元，比 2019 年增长 9.6%，增速位居世界第一，规模位居世界第二。〔1〕我国数字经济规模无论在增速还是体量上都在全球范围内位居前列。但是，我国的数字经济规模与我国在全球数字贸易中的话语权并不匹配，亟需构建兼顾数字产业特点和我国诉求的“中国方案”。〔2〕2021 年 10 月 30 日，习近平在 G20 领导人第十六次峰会上提

* 靳思远，上海交通大学法学院博士研究生。

本文为 2021 年国家社科基金重大项目“美国全球单边经济制裁中涉华制裁案例分析与对策研究”（21&ZD208）的阶段性成果。

〔1〕 参见中国信息通信研究院：《全球数字经济白皮书——疫情冲击下的复苏新曙光》，载 http://www.caict.ac.cn/kxyj/qwfb/bps/202108/P020210913403798893557.pdf，最后访问时间：2022 年 1 月 8 日。

〔2〕 参见赫璟、陈紫媛：《DEPA 协定有利于数字规则“中国模板”的构建》，载《国际商报》2022 年 2 月 15 日，第 7 版。

出，中国决定申请加入《数字经济伙伴关系协定》（Digital Economy Partnership Agreement，简称 DEPA）。〔3〕2021 年 11 月 1 日，中国商务部部长代表中方向 DEPA 保存方新西兰正式提出加入 DEPA 申请。〔4〕2022 年 2 月 17 日，中国商务部发言人表示，中方现阶段正与 DEPA 缔约方开展沟通和技术磋商，中方希望为 DEPA 成员国企业提供合作机遇和广阔的市场，并在创新和可持续发展等方面作出中国贡献。〔5〕

中国的申请加入可能使 DEPA 在未来的全球数字经济规则框架中占据更为主流的地位，而 DEPA 作为开放性的数字经济协定为中国参与全球数据治理提供了一种新的路径。本文通过分析全球数据治理格局和 DEPA 的数据相关议题，结合中国数据出境评估体系的制度现状，探究中国加入 DEPA 在数据治理方面可能带来的机遇和挑战。

一、全球数据治理格局

随着全球数字化进程的推进，传统贸易逐渐向数字化趋势发展。数据作为数字经济的基础性资源和不可或缺的生产要素，被视为数字经济深化发展的核心引擎。〔6〕以信息技术驱动的全球数字贸易在很大程度上依赖于数据的跨境流动。在倡导“规则的设定应围绕资源的有效配置和合理利用展开，以追求制度效率的最大化”的法经济学视角下，〔7〕数据实际上构成了一种固定于一定载体上，能够满足人们生产和生活需要，具有确定性、可控制性、独立性、价值性和稀缺性等特征的信息财产。〔8〕从信息主体的角度看，数据作为个人信息的重要载体，又关系到个人隐私保护和人格利益。因此，数据兼具财产利益和人格利益，在数据治理中分别对应数据流动和数据安全。前者强调数据在数字交易中的经济价值和商业价值，后者强调通过法律保护个人隐私和信息安全。不同国家基于本国对数据技术掌控的能力、经济制度和经济发展等因素的影响，产生了不同的规制路径并影响其参与全球博弈的立场，分歧在所难免。在 WTO 多边数字贸易治理体系无法取得突破性进展的背景下，各国治理数据的路径呈现多元化态势，〔9〕全球数据治理格局具有复杂性的特征。其中，美国与欧盟两个发达经济体之间的跨境数据流动量位居世界首位，双方在数字贸易、隐私和国家安全方面的不同做法已经对美欧之间的数据流动造成一定的阻碍。这种阻碍尤其体现在 Schrems 系列案件〔10〕中，用于跨大西洋数据传输的法律依据——“安全港协议”“隐私盾协议”——均被欧盟法院判定无效。美欧通过国内法的“长臂管辖”和与他国区域

〔3〕 参见新华网：《习近平在二十国集团领导人第十六次峰会第一阶段会议上的讲话》，载 http://www.xinhuanet.com/world/2021-10/30/c_1128013842.htm，最后访问时间：2022 年 1 月 8 日。

〔4〕 参见人民网：《中方正式提出申请加入〈数字经济伙伴关系协定〉》，载 http://finance.people.com.cn/n1/2021/1101/c1004-32270753.html，最后访问时间：2022 年 1 月 9 日。

〔5〕 参见文汇网：《中方目前正按照 CPTPP 有关加入程序，与各成员进行接触磋商》，载 https://www.whb.cn/zhuzhan/rd/20220217/450203.html，最后访问时间：2022 年 1 月 9 日。

〔6〕 参见沈伟、赵尔雅：《数字经济背景下的人工智能国际法规制》，载《上海财经大学学报》2022 年第 5 期。

〔7〕 See Richard A. Posner, *Economic Analysis of Law*, Aspen Law & Business, 1998, p. 3.

〔8〕 参见齐爱民：《捍卫信息社会中的财产》，北京大学出版社 2009 年版，第 53-54 页。

〔9〕 参见齐俊妍、强华俊：《数据流动限制、数据强度与数字服务贸易》，载《现代财经》2022 年第 7 期。

〔10〕 参见单文华、邓娜：《欧美跨境数据流动规制：冲突、协调与借鉴——基于欧盟法院“隐私盾”无效案的考察》，载《西安交通大学学报（社会科学版）》2021 年第 5 期。

贸易协定中数字贸易规则的谈判，试图将带有本国利益色彩的国内法推广至国际规则层面。

以《跨太平洋伙伴关系协定》（Trans-Pacific Partnership Agreement，简称 TPP）电子商务章、《美墨加协定》（The United States-Mexico-Canada Agreement，简称 USMCA）数字贸易章为代表的“美式规则”强调贸易便利化、跨境数据自由流动、免收数字关税、源代码开放等内容，其主张构建开放自由的全球数字市场。从数字经济发展历史看，美国作为互联网的发源地，无论是互联网企业的数量还是信息产业发达程度都领先全球，互联网科技巨头在早期更是可以轻而易举地从他国获得大量数据信息。因此其政策具有准入严格而监管相对松弛的特性，主张数字贸易自由化和便利化。从美国国内法上看，个人数据被包含在隐私保护的框架内，但没有类似欧盟《一般数据保护条例》（General Data Protection Regulation，简称 GDPR）的关于隐私保护的综合性法律，而是分散在各种行业的合同相关法律上。〔11〕美国的隐私保护主要由数据处理者和隐私消费者之间的合同提供，并由美国联邦贸易委员会监督。〔12〕但事实上，由于缔约双方之间的权力和信息不对称，个人数据并不能得到充分的保护。虽然美国联邦最高法院通过其判例确认公民享有个人数据的宪法保护权利，但各级法院一般都避开了这一决定。最高法院对宪法的解释是赋予个人隐私权，但这一权利通常只是为了防止政府对公民隐私的侵犯。〔13〕虽然美国目前没有专门规制跨境数据流动的法律，但对个人敏感数据、政府重要数据、商业数据等数据出境有着较为严格的管控要求。美国尤其关注外国产品或服务中收集、获取美国敏感数据的风险，并以国家安全为由对外国产品或服务进行较为严格的管控。例如，特朗普政府在执政期间以国家安全为由，通过行政令等方式意图驱逐或封杀 TikTok，施压其母公司字节跳动放弃对 TikTok 的所有权。拜登上台后通过颁布一系列针对信息及通信技术和服务供应链审查规则（ICTS 规则）的行政令，进一步强化了对跨国科技企业的安全审查。总体而言，美国在数据治理中秉持“全球主义”理念，既通过国内法限制公权力对数据流动的干预，又倡导“私法自治”，赋予私主体在保护个人权利和创造商业价值之间更大的选择权。〔14〕但在国际投资领域，美国又以维护国家安全为由对外国数据控制者在美国国内的经营活动进行严格审查，以消除跨境数据流动对美国国家安全可能带来的威胁。虽然“美式规则”主张构建开放自由的全球数字市场，但 USMCA 针对非市场经济国家的“毒丸条款”〔15〕和“美式规则”对数字市场开放的高水平要求一定程度上加深了与发展中国家之间的“数字鸿沟”，以“美式规则”作为全球数字治理方案仍然存在诸多阻碍。

不同于美国的“全球主义”，欧盟在数据治理方面主张建立数字单一市场，数据可以在该市场内部自由流通并受到欧盟数字法规的严格保护，而数据的跨境流动也会受到较为严格的限制。欧盟拥有目前最严格的数据保护规则，根据 2000 年《欧盟基本权利宪章》（Charter of Funda-

〔11〕 See Zheng Guan，Trilemma and Tripartition：The Regulatory Paradigms of Cross-Border Personal Data Transfer in the EU，the U. S. And China，43 *Computer Law & Security Review* 5 (2021).

〔12〕 参见前引〔11〕，Zheng Guan 文。

〔13〕 例如 1978 年的《美国隐私法》（U. S. Privacy Act）规定了联邦政府如何管理其拥有的个人信息，1986 年的《电子通信隐私法》（Electronic Communications Privacy Act）扩大了政府对电话窃听的限制，包括对电脑传输电子数据的限制。

〔14〕 参见沈伟、冯硕：《全球主义抑或本地主义：全球数据治理规则的分歧、博弈与协调》，载《苏州大学学报（法学版）》2022 年第 3 期。

〔15〕 非市场经济条款，又称“毒丸条款”，即禁止与美国有自贸协定的贸易伙伴与非市场经济国家签订自贸协定。参见沈伟：《“修昔底德”逻辑和规则遏制与反遏制——中美贸易摩擦背后的深层次动因》，载《人民论坛·学术前沿》2019 年第 1 期。

mental Rights of European Union）第7条〔16〕和第8条，〔17〕通信隐私和个人数据保护是欧盟国家公民的基本权利。基于人权保护，欧盟主张以本地化存储和数据跨境审核为核心的数据“本地主义”。欧盟通过提高跨境数据输出的审查标准及“长臂管辖”制度，〔18〕试图将GDPR建立的“欧盟数字标准”推广成世界标准。〔19〕欧盟数据保护规则适用于欧洲经济区（European Economic Area，简称EEA），其中包括所有欧盟国家和非欧盟国家冰岛、列支敦士登和挪威。欧盟在2016年4月通过改革数据保护立法，赋予个人更多对其个人数据的控制权，提供了将数据传输到第三国的多样化工具，包括“充分性决定”“标准合同条款”“具有约束力的公司规则”等等。其中，“充分性决定”用来确定非欧盟国家提供的数据保护水平与欧盟“基本相同”，其效果是使个人数据能够自由流动到该第三国，而无需数据出口商提供进一步的保障或获得任何授权。在不满足“充分性决定”要求的情况下，数据跨境流动可以在提供适当数据保护保障的其他替代转移工具的基础上进行。其中，“标准合同条款”被应用于欧盟加工商与非欧盟国家加工商之间的合同中，“具有约束力的公司规则”作为跨国公司集团采用的内部规则，用于在同一公司集团内向位于未提供足够保护水平的国家或地区的实体进行数据传输，也可以由从事联合经济活动的一组企业使用。欧盟通过自身市场在国际市场的中枢地位，借助强势的域外管辖立法，其严格的数据规制才能发挥所谓的“布鲁塞尔效应”（Brussel effect），〔20〕其他国家若想和欧盟进行数据交流必须“迎合”其“充分保护原则”下的严格条件。以GDPR为代表的欧盟数据保护法律框架也经常作为第三国制定该领域立法的参考点，欧盟同时在双边和多边层面积极与其国际合作伙伴进行对话，通过在全球范围内制定严格且可互操作的个人数据保护标准来促进数字贸易。

美欧基于对数据财产利益和人格利益的保护倾向不同，产生了“全球主义”和“本地主义”的治理理念分歧。而数字经济发展的新兴国家基于各自对数据属性的不同认识和本国国情而倾向于不同的数据治理理念。以俄罗斯、印度为代表的发展中国家倾向于“本地主义”，强调基于人权与主权的数据保护。俄罗斯既要求跨国企业在俄开展业务或提供服务时须在俄境内建立数据中心，也对数据存储和服务器地址提出本地化要求，总体上采取“孤岛式”的数据规制路径。〔21〕印度作为一个民族国家，将其公民产生的数据视为国家资产，在国界内存储和保护这些数据来维护其国防和战略利益。《印度电子商务国家政策框架草案》提出，印度将会逐步推进数据本地化政策并建立数据中心。〔22〕而以新加坡为代表的发达国家更倾向于“全球主义”，强调数据的跨境

〔16〕《欧盟基本权利宪章》第7条“尊重私人和家庭生活”规定：“人人均有权要求尊重其私人与家庭生活、住居及通信信息。”

〔17〕《欧盟基本权利宪章》第8条“个人数据的保护”规定：“1. 人人均有权保护其个人信息；2. 这些信息仅于特定目的，并且在信息所有人同意或法律规定的其他合法基础上公平处理，人人均有权查阅其个人信息，并有权要求纠正其信息；3. 这些规则的遵守应当受到独立机关的控制。”

〔18〕根据GDPR第3条“地域范围”的相关规定，即便数据控制者或处理者在欧盟境内没有设立实体机构，但其对数据主体的个人数据处理行为，即适用该法。参见叶开儒：《数据跨境流动规制中的“长臂管辖”——对欧盟GDPR的原旨主义考察》，载《法学评论》2020年第1期。

〔19〕参见前引〔18〕，叶开儒文。

〔20〕参见彭岳：《数字贸易治理及其规制路径》，载《比较法研究》2021年第4期。

〔21〕参见孙祁、〔俄〕尤利娅·哈里托诺娃：《数据主权背景下俄罗斯数据跨境流动的立法特点及趋势》，载《俄罗斯研究》2022年第2期。

〔22〕参见陈志：《亚洲国家数据跨境流动的实践及对我国的启示》，载《北京金融评论》2020年第1期。

流动和开放合作。除 DEPA 外，新加坡还分别与澳大利亚、英国签署了专项数字经济协定，这些数字经济协定鼓励国内监管改革和在数据创新、数字身份、网络安全等广泛问题上的跨境合作。2021 年 1 月 22 日，第一次东南亚国家联盟（ASEAN）数字部长会议批准了《东盟数据管理框架》（DMF）和《跨境数据流动示范合同条款》（MCC），[23] 提出要建立东盟数据跨境流动机制并减少不必要的限制，这些文件都是由新加坡主持的数据治理工作组所制定。通过这些数字经济协定和多边安排，新加坡正逐步构建其主导的数字经济联盟及次级伙伴关系，为发展本国数字贸易、开展中小企业合作打下基础，为未来构建国际数字规则的谈判争取更大的话语权。

二、DEPA：全球数据治理的新路径

WTO 电子商务诸边谈判目前提案及进展表明，各成员的数字产业和贸易政策有很大不同，短期内难以达成一致的全球数字治理方案。数据是数字贸易和更广泛的数字经济的核心。美欧分别基于数字技术和数字市场的比较优势，在数据规制方面具有不同的理念和路径，并积极推进国内数字规则的国际法化。在此背景下，DEPA 作为世界首个专门针对数字经济、为促进数字贸易合作而制定的多边协定，其开放性的模块化框架和多元化的内容成为有别于美欧数字治理、反映中小国诉求的一种新路径，相较传统的数据治理路径更具有灵活性和可扩展性。从内容上看，无论是个人信息保护和跨境数据流动（模块 4）等争议性数据问题，还是数据创新（模块 9）、数字包容（模块 11）等新兴议题，都体现出新加坡等中小国家在数据治理问题上的开放性理念和规制路径，鼓励成员国之间可信数据（trusted data）的安全流动。

（一）争议性数据问题：“美式规则”基础上的调整和更新

美欧在数字贸易规则传统性议题上的矛盾和分歧体现在数据流动和个人信息保护等相关问题的处理上，这些问题集中体现在 DEPA 的模块 4 中，分别涉及个人信息保护（第 4.2 条）、跨境数据流动（第 4.3 条）和计算设施的位置（第 4.4 条）。

在个人信息保护问题上，DEPA 第 4.2 条构建了 10 条规则，从倡导性规则、构建个人信息保护相关法律应该考虑的关键原则、非歧视性原则及信息保护公开、信息保护机制的兼容性和数据保护信任标志等方面，对缔约方在个人信息保护方面提出了全面且兼具深度的承诺要求。TPP 第 14.8 条和 USMCA 第 19.8 条都对个人信息保护做了相关规定，两者和 DEPA 在倡导性规则、非歧视性原则及信息保护公开方面具有高度的重合性。具体而言，三者都强调保护数字用户个人信息的经济和社会效益，缔约国应考虑个人信息保护相关国际机构的原则和指南以制定本国的法律框架，采取非歧视性做法，从个人和企业层面公布其向数字贸易用户提供的个人保护信息。关于构建个人信息保护相关法律应该考虑的关键原则，TPP 未有提及，而 USMCA 作为“美式规则”的升级版提出了“限制收集、选择、数据质量、目的规范、使用限制、安全保障措施、透明度、个人的参与、问责制”共九个原则，并“确保对个人信息跨境流动的任何限制是必要的，并

〔23〕 参见中国商务部：《东盟发布〈东盟数据管理框架〉和〈东盟跨境数据流动示范合同条款〉》，载 http://asean.mofcom.gov.cn/article/jmxw/202102/20210203036591.shtml，最后访问时间：2022 年 8 月 2 日。

与所涉风险相称”〔24〕，即任何限制不能超过保护个人数据所需的要求。这种与隐私风险相称的必要限制正是“全球主义”的直接体现，与欧盟“本地主义”采取严格保护个人隐私的限制性措施不同，即前者的限制是例外、后者的限制是原则。DEPA借鉴了USMCA除“选择”外的其他八个关键原则，但没有规定对个人信息跨境流动进行限制要遵守必要性原则，即在个人信息跨境流动的限制问题上做了保留。即便DEPA缔约国可以选择加入某一主题模块而无需一揽子同意，但从条文上来看，DEPA在个人信息跨境流动问题上没有在“全球主义”和“本地主义”之间选边站，也一定程度上展现了新加坡等中小国家在此类争议性问题上的折中态度。

在跨境数据流动的问题上，DEPA第4.3条与TPP第14.11条内容一致，通过三项规定，承诺有约束力的跨境数据自由流动。这种约束力体现在条文中“shall”“may”等情态动词的使用，“shall”表达的是法律的强制性，“may”传递的是法律的授权性。〔25〕第一项采用“may”授权缔约国对跨境数据流动有本国的监管要求。第二项和第三项均采用“shall”，要求缔约国既要允许跨境数据流动，也可以在不构成“不合理歧视或贸易限制”或“过度采取管制”的前提下，采用出于“合法公共政策目标”的跨境数据流动管制措施，这保留了缔约方对“跨境数据自由流动”进行管制的自主空间。〔26〕相较而言，USMCA第19.11条只保留了上述第二、三项内容，没有授予其他缔约方设置本国监管要求的权限，即没有监管例外规定。类似地，在计算设施的位置问题上，DEPA第4.4条与TPP第14.13条内容一致，要求不得强制将数据存储设施设置在当地，并规定了监管例外和公共安全例外。而USMCA第19.12条仅规定了“任何一方不得要求被覆盖人员在其领土内使用或放置计算设施，以此作为在该领土内开展业务的条件”，没有其他例外规定。在一般例外条款方面，DEPA第15.1.3条将《服务贸易总协定》（GATS）第14条和《1994年关税与贸易总协定》（GATT1994）第20条的所有内容纳入规则范围，而TPP第29.1.3条和USMCA第32.1.2条仅将GATS第14条（a）—（c）纳入规则范围，排除了（d）（e）与最惠国待遇和国民待遇相冲突的两种情况以及GATT1994第20条列举的一般例外适用情形。通过对比DEPA、TPP和USMCA的数据规制条文不难发现（如表1所示），DEPA除了避开“与隐私风险相称的必要限制”的争议性原则，首倡数据保护信任标志的国际合作，其他事项都充分借鉴了TPP电子商务章和USMCA数字贸易章的“美式规则”。但DEPA在数据规制上的例外规定范围明显大于USMCA，这也说明了USMCA较DEPA具有更高的开放度，DEPA也更加侧重保护缔约方的监管权限。从新加坡等中小国家的发展来看，这种对数据跨境流动相对保守的态度是出于对本国中小企业发展的保护。以美国为代表的“全球主义”国家坚持数字贸易自由化，试图最大限度地消除各国数字贸易进入障碍，为其优势数字企业扩大市场份额提供便利，数字贸易相对落后的国家则希望通过设置保护壁垒为本土数字企业发展赢得成长空间。

〔24〕 USMCA Article 19.8.3.

〔25〕 参见王子颖：《法律语篇中shall和may的翻译对比研究》，载《上海翻译》2013年第4期。

〔26〕 参见陈寰琦、陆锐盈：《DEPA数据安全规则解析及对中国的启示》，载《长安大学学报（社会科学版）》2022年第2期。

表 1 DEPA、TPP 和 USMCA 数据规制相关条文对比

事项	DEPA	TPP	USMCA
个人信息保护	在倡导性规则、鼓励缔约方发展兼容的信息保护机制、非歧视性原则及信息保护公开等方面较为一致		
	第 4.2.3 条规定了 8 个关键原则，没有规定对个人信息跨境流动进行限制要遵守必要性原则	未规定制定法规的关键原则	第 19.8.3 条规定了 9 个关键原则和“与隐私风险相称的必要限制”原则
	第 4.2 条 8—10 款鼓励缔约方就数据保护信任标志展开合作	未规定数据保护信任标志相关内容	
跨境数据流动	DEPA 第 4.3 条与 TPP 第 14.11 条内容一致，都承诺有约束力的跨境数据自由流动，并规定了监管例外和公共安全例外		没有监管例外
计算设施的位置	DEPA 第 4.4 条与 TPP 第 14.13 条内容一致，要求不得强制将数据存储设施设置在当地，并规定了监管例外和公共安全例外，保留监管自主空间的权限		USMCA 第 19.12 条仅保留了推动数据流动自由化的条款，没有监管例外和公共安全例外
一般例外条款	DEPA 第 15.1.3 条将 GATS 第 14 条和 GATT1994 第 20 条的所有内容纳入规则范围，较 TPP 和 USMCA 更广泛	TPP 第 29.1.3 条和 USMCA 第 32.1.2 条都要求针对“数字贸易”或“电子商务”章节，仅参考 GATS 第 14 条（a）（b）（c）的要求进行例外条款修订	

表格来源：作者整理。

（二）新兴数据议题为全球数据治理提供了中小国方案

除了传统性的数据议题，DEPA 还提出了一系列创新性的数据议题，为全球数据治理提供了最新的关注点。首先，在数字贸易便利化方面，DEPA 首倡电子发票、物流和快递等议题，提倡缔约国努力实现数据交换系统的互联互通，努力构建国际公认的数据开放标准，以提升数字贸易的效率、降低交易成本。其次，DEPA 要求缔约方认识到在个人或企业数字身份方面的合作将有利于区域和全球互联互通，构建数字身份的安全和可互操作的标准会使消费者因数字身份被欺诈案件减少，企业受益于电子方式可以进行更高效的交易。再次，跨界数据流动和数据共享能够实现数据驱动的创新，DEPA 鼓励缔约国通过监管“沙盒”等方式进行合作，实现跨国界的数据驱动创新以促进新产品和服务的开发。中小企业也应当通过创建免费且可公开访问的网站实现跨国企业之间信息的互联互通，通过举办数字中小企业对话等活动促进企业合作。最后，DEPA 鼓励缔约国开放政府数据，便利公众获取和使用政府信息可促进经济和社会发展、竞争力提升和创新。政府开放的数据是政府部门掌握的没有经过加工处理的原始数据，政府数据开放的真正意义在于对这些数据进行共享和利用。〔27〕缔约方应努力开展合作，以确定缔约方可扩大获取和使用公开数据的方式，以期增加和创造商业机会。此外，DEPA 还提倡在金融科技、人工智能等领域展开数据方面的交流和合作。

然而，上述倡议性的新兴数据议题大多都是鼓励缔约国展开合作，并没有具有可操作性的方

〔27〕 参见李涛：《政府数据开放与公共数据治理：立法范畴、问题辨识和法治路径》，载《法学论坛》2022 年第 5 期。

案。例如，在金融科技领域，DEPA 鼓励双方在行业层面的合作，但事实上这种合作是基于双方国内金融机构控制的数据和信息交流，DEPA 并没有规定金融数据相关的市场准入问题，很可能会使这样的倡议流于形式。相较而言，《英国—新加坡数字经济协议》（The UK-Singapore Digital Economy Agreement，简称 UKSDEA）对金融部门的跨境数据流动有着更明确的要求，〔28〕英新两国之间金融数据的流通就有了更强的非歧视性待遇保证。另外，DEPA 认识到监管“沙盒”对数据创新的重要性，但是并没有对数据开放等实质性问题提出解决方案，例如怎样平衡数据流动和个人信息保护之间的冲突，在政府、数字企业、个人之间关于数据方面的权利义务分配上坚持怎样的原则等。可见，DEPA 虽然在这些创新性议题上表达了中小国家在数字贸易方面的利益诉求，但这种诉求仍然是宏观且宽泛的，仍需进一步构建具有可操作性的方案。

三、DEPA：数据治理的中国选择

中国经济正处于迈向高质量发展新阶段的关键期，以新基建为主要引擎的数字化转型发展战略持续深入推进。〔29〕目前，中国尚未形成具有鲜明特征的数字贸易规则主张，这主要是由于我国将数据流动置于国家安全的考量范围，突出了安全风险。在数字贸易规则深入性议题方面，我国呈现出较为保守的态度，在规则国际博弈中处于防守地位。〔30〕我国数字贸易比较优势主要集中在基于互联网平台的货物贸易，因此在参与 WTO 电子商务诸边谈判时，我国的提案主要侧重于跨境货物贸易及相关支付和物流服务方面，如电子认证、电子合同等贸易便利化层面促进电子商务的传统议题。〔31〕我国在最近的一份公开性提案中提出，对于数据流动、数据存储、数字产品处理等敏感和复杂的问题，需要进行更多的探索性讨论。〔32〕但在原则上，数据流动应当以安全为前提，数据安全关系到每个 WTO 成员核心利益，所以有必要按照各国法律法规进行有序的数据流动。〔33〕我国目前已签署的双边自由贸易协定（Free Trade Agreement，简称 FTA）电子商务章节中的条款大多数是在 WTO 框架下早已达成共识的传统条款。例如，中国与 DEPA 的三个发起国都分别签订了 FTA 且均包含电子商务章，但内容局限于无纸化贸易、关税、透明度义务、在线消费者保护等内容，在具有争议的个人信息保护议题方面大多只是强调个人信息保护的重要性、制定相关法律要考虑相关国际组织或机构的标准等“倡议性”规定。

此次申请加入 DEPA 表明我国在全球数据治理中的路径选择，即接受 DEPA 基于中小国家

〔28〕 例如，UKSDEA 第 8.53.1 条规定：“每一方均应允许另一方的金融服务供应商提供甲方允许其同类金融服务供应商提供的任何新的金融服务，而无需甲方要求采取额外的立法行动。各缔约方可确定提供新金融服务的机构和司法形式，并可要求获得提供该服务的授权。如果一方要求此类授权，则应在合理的时间内作出决定，且仅可根据第 8.50 条（审慎剥离）的审慎理由拒绝授权。”第 8.54.1 条规定：“在遵守适当的隐私和保密保障措施的前提下，如果此类转移是在该金融服务供应商的正常业务过程中需要的，任何一方不得禁止或限制另一方的金融服务供应商将电子或其他形式的信息转移到或转移出其领土。”

〔29〕 参见腾讯网：《中国申请加入 DEPA 的九大看点》，载 https://new.qq.com/omn/20211103/20211103A06IX500.html，最后访问时间：2022 年 2 月 10 日。

〔30〕 参见朱福林：《数字贸易规则国际博弈、“求同”困境与中国之策》，载《经济纵横》2021 年第 8 期。

〔31〕 参见李馥伊：《构建高标准自贸区网络的对策分析》，载《中国经贸导刊》2019 年第 17 期。

〔32〕 参见卢锋、李双双：《多边贸易体制应变求新：WTO 改革新进展》，载《学术研究》2020 年第 5 期。

〔33〕 See WTO，Joint Statement on Electronic Commerce-Communication from China，INF/ECON/40，Article 4.3.

数字经济发展诉求的理念和规则。在新冠疫情给国际贸易供应链造成了严重破坏的背景之下，包括中国和 DEPA 发起国在内的各国企业发展遭遇瓶颈，亟需有效的数字化转型战略和合作平台。DEPA 在发展数字经济领域具有更强的灵活性和专业性，人工智能、中小企业合作等创新性议题的引入更是增加了协定的前瞻性，与中国未来创新经济发展与转型的趋势、“坚持包容普惠、推动共同发展”〔34〕的理念相契合。国务院《“十四五”数字经济发展规划》指出，发展数字经济要“统筹发展和安全、统筹国内和国际”。〔35〕中国申请加入 DEPA 意味着在数字领域推动国内治理和国内法规向高标准数字规则看齐，并且考量 DEPA 在数字方面的某些规则，建立国内数据市场和数字贸易治理的标准，实现“两个统筹”。

约翰·杰克逊（John H. Jackson）教授的“接合”（interface）理论提出，两个国家即使只有很小的经济制度差异，它们在进行合作时必须有一种“接合”机制，否则就会发生摩擦或误解。〔36〕这种“接合”机制必须具备一定的开放性、包容性和灵活性，才能使不同经济制度的国家在同一个问题达成共识和合作。DEPA 从灵活开放的模块式框架结构到多元包容的数字议题，都具备国际数字经济规则的“接合”特性，以便不同国家在多元化的数字议题上寻求共识。对标 DEPA 高标准的数字贸易规则，能够在一定程度上倒逼我国加快数字经济领域建章立制的进度，对我国国内数字法规产生积极的“接合”作用。

推动数据跨境安全流动是 DEPA 的传统性议题的核心内容之一，我国申请加入 DEPA 也意味着我国在数据跨境流动问题上接受 DEPA 的规则和理念。从目前正在构建的数据出境评估体系来看，我国国内法在跨境数据流动问题上仍然秉持十分审慎的态度。虽然 DEPA 没有规定个人信息跨境流动限制要遵守必要性原则，但我国的态度与 DEPA 总体上鼓励数据跨境自由流动、政府数据开放共享等相对宽松的理念仍然存在一定的张力。

（一）构建中国数据出境评估体系

我国近年密集出台《网络安全法》《数据安全法》《个人信息保护法》等数字经济相关的多部法律法规，也在一些试验区试点企业数据分类和跨境流动。但目前国内的相关政策和法规与 DEPA 相比仍存在差距，偏重强调数据的安全属性和数据本地化要求。《个人信息保护法》严格规范了个人信息的存储、传输和处理，对国家安全构成潜在威胁的信息跨境传输将受到限制，第 36 条针对国家机关处理的个人信息设置了“境内存储为原则、安全评估后出境为例外”的原则，〔37〕在数据流动和数据安全中更倚重后者，以数据本地化存储为原则。第 38 条第 1 款规定个

〔34〕 中国政府网：《坚持包容普惠，推动共同发展——论习近平主席在首届中国国际进口博览会开幕式上主旨演讲》，载 http://www.gov.cn/xinwen/2018-11/07/content_5338282.htm，最后访问时间：2022 年 7 月 26 日。

〔35〕 参见中国政府网：《“十四五”数字经济发展规划》，载 http://www.gov.cn/zhengce/zhengceku/2022-01/12/content_5667817.htm，最后访问时间：2022 年 7 月 23 日。

〔36〕 这种“接合”（interface）机制借用了计算机术语。当需要两台不同机器的计算机一起工作时，通常需要某种“接口”机制或程序在它们之间进行调解。约翰·杰克逊教授认为，国家贸易法和关贸总协定-布雷顿森林体系如今是作为一种相当粗糙的（crude）“接合”机制运作的。See John H. Jackson, Import Practices: Are They Really Unfair?, 30 *Law Quadrangle* 26 (1986).

〔37〕《个人信息保护法》第 36 条规定：“国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行安全评估。安全评估可以要求有关部门提供支持与协助。”参见彭錞：《论国家机关处理的个人信息跨境流动制度——以〈个人信息保护法〉第 36 条为切入点》，载《华东政法大学学报》2022 年第 1 期。

人信息跨境提供必须具备下列四个条件之一，即“（1）通过国家网信部门组织的安全评估；（2）按照国家网信部门的规定经专业机构进行个人信息保护认证；（3）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；（4）法律、行政法规或者国家网信部门规定的其他条件”。为使上述个人信息出境条件落地，除第四项兜底条款，国家网信部门近期分别发布了《数据出境安全评估办法》（简称《评估办法》）〔38〕《网络安全标准实践指南——个人信息跨境处理活动安全认证规范》（简称《安全认证规范》）〔39〕和《个人信息出境标准合同规定（征求意见稿）》（简称《标准合同规定》），〔40〕对前三个条件分别予以细化。其中，《评估办法》全面系统地提出了我国数据出境安全检查的具体要求，也标志着我国数据出境安全评估制度的正式落地。

从适用范围来看，《评估办法》第 4 条规定了数据处理者向境外提供数据〔41〕必须申报安全评估的四种情形：“（1）数据处理者向境外提供重要数据；（2）关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息；（3）自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息；（4）国家网信部门规定的其他需要申报数据出境安全评估的情形。”关于“重要数据”的定义，《评估办法》第 19 条首次从部门规章层面予以明确，即指“一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据”。但该定义事实上掺杂着地缘政治因素，何种数据能够被认定为“可能危害”国家安全等并没有清晰的标准和边界，存在一定的模糊性，给予审查部门较大的主观裁量空间。《评估办法》适用范围外的个人信息处理者的数据出境情形，可以通过个人信息保护认证或者签订国家网信部门制定的标准合同来满足个人信息跨境提供条件，依法开展数据出境活动。〔42〕从评估内容和评估流程来看，《评估办法》第 5 条和第 9 条分别列举了数据处理者开展数据出境风险自评估的重点事项、与境外接收方订立的法律文件中数据安全保护责任义务主要内容，第 8 条列举了网信部门开展数据出境安全评估的重点事项，为数据处理者开展数据出境风险评估提供更具有可操作性的指导。

由表 2 可见，相较于申报人风险自评估的内容，网信部门安全评估重点事项与其基本一致，都包括了出境数据的基本要求、数据出境活动可能带来的风险、境外接受方数据保护水平、数据出境中和出境后的评估、境外接受方的数据安全保护责任义务等内容。安全评估重点事项在此基础上还增加了对境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境的评估，以及对数据处理者遵守中国法律、行政法规、部门规章情况的评估，充分体现了数据出境“风险

〔38〕 参见国家互联网信息办公室：《数据出境安全评估办法》，载 http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm，最后访问时间：2022 年 7 月 24 日。

〔39〕 参见全国信息安全标准化技术委员会：《网络安全标准实践指南——个人信息跨境处理活动安全认证规范》，载 https://www.tc260.org.cn/upload/2022-06-24/1656064151109035148.pdf. 最后访问时间：2022 年 7 月 24 日。

〔40〕 参见国家互联网信息办公室：《个人信息出境标准合同规定（征求意见稿）》，载 http://www.cac.gov.cn/2022-06/30/c_1658205969531631.htm，最后访问时间：2022 年 7 月 24 日。

〔41〕《评估办法》所称数据出境活动主要包括：一是数据处理者将在境内运营中收集和产生的数据传输、存储至境外；二是数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以访问或者调用。

〔42〕 参见人民网：《〈数据出境安全评估办法〉答记者问》，载 http://politics.people.com.cn/n1/2022/0707/c1001-32469307.html，最后访问时间：2022 年 7 月 24 日。

表 2　　数据出境风险自评估、安全评估及境外接受方数据安全保护责任义务内容比较

主要内容	自评估重点事项（第 5 条）	网信部门评估重点事项（第 8 条）	与境外接收方约定数据安全保护责任义务（第 9 条）
出境数据的基本要求	（一）数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；（二）（1）出境数据的规模、范围、种类、敏感程度	（一）数据出境的目的、范围、方式等的合法性、正当性、必要性；（三）（1）出境数据的规模、范围、种类、敏感程度	（一）数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等
数据出境可能带来的风险	（二）（2）数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险	数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险	无（以责任承担的方式呈现）
境外接收方的数据保护水平	（三）境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全	（二）（2）境外接收方的数据保护水平是否达到中国法律、行政法规的规定和强制性国家标准的要求	（二）数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施；（三）对于境外接收方将出境数据再转移给其他组织、个人的约束性要求
数据出境中和出境后的评估	（四）数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等	（三）（2）出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险； （四）数据安全和个人信息权益是否能够得到充分有效保障	（六）出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式
境外接收方的数据安全保护责任义务	（五）与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等是否充分约定了数据安全保护责任义务	（五）数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务	（四）境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施；（五）违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式
其他	无	（二）（1）境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；（六）遵守中国法律、行政法规、部门规章情况	无

表格来源：作者整理。

自评估与安全评估相结合”的严格原则。《评估办法》第 9 条“与境外接收方约定数据安全保护责任义务”与两者要求大体一致，《标准合同规定》中的合同模板第三条“境外接收方的义务”就是在第 9 条的基础上展开的。《评估办法》第 4 条项下的四类情形作为审查对象，只有通过安全评估、获得“行政许可”才能有出境的资格，体现出监管部门对这四类情形安全评估十分审慎的态度。另外，《评估办法》第 14 条〔43〕和第 17 条〔44〕规定了数据出境安全评估的结果具备两年有效期及需要重新申报评估的情形，不符合要求则会被书面通知终止数据出境活动，体现了“事前评估和持续监督相结合”的原则。而对于《评估办法》第 4 条的四类情形之外的数据出境，由于没有达到安全评估的“门槛”则只需要按照《个人信息保护法》第 38 条第 2 或第 3 项得到专业机构个人信息保护认证或与境外接收方订立标准合同，即可进行数据出境。相较于数据出境安全评估的流程，标准合同这种出境路径更加快捷、可预期、成本低，虽然合同签署后需要在网信部门备案，但备案不作为合同生效条件和信息出境的前置条件；认证机制的适用为跨国公司或者同一经济、事业实体内部的个人信息跨境处理活动提供“绿色通道”。在《网络安全法》《数据安全法》《个人信息保护法》等法律作为上位法、《评估办法》等部门规章作为下位法的国内数据法律体系下，我国正在逐步建立“安全评估审查下的高风险数据有限流动、标准合同和认证机制下的低风险数据自由流动”的数据出境评估体系。

（二）缓解国内数据规则与 DEPA 之间的张力

如前文所述，我国对于《评估办法》第 4 条的四类高风险数据出境采取“无授权则不可为”的行政许可模式，对其他低风险数据采用标准合同和认证机制的处理模式，这些模式实质上都属于数据本地化范畴，即只有符合要求才能允许数据出境，否则只能在本地存储。数据本地化作为严格限制跨境数据流动的一种属地规制模式，“将地域性的传统主权观念照搬至全球性的现代数字经济，容易产生安全与发展之间方枘圆凿的冲突”〔45〕。《评估办法》等配套规则生效后，相关企业和个人发起的任何数据跨境传输活动都必须与境外数据接收方签署上述具有法律效力的文件，给接收方施加种种义务并进行一系列谈判，经济和时间成本可能会随之增加。统筹数字经济的发展和安全，体现在跨境数据流动中就是要在数据的高效流动和安全稳定之间寻找平衡点。数据出境评估体系也应当根据实践予以调整，在保障数据安全出境的前提下，减少不必要的行政程序，明确审查规则，提高数据跨境流动的效率。

中国已加入的《区域全面经济伙伴关系协定》（RCEP）在“电子商务”章明确了电子商务项

〔43〕《评估办法》第 14 条规定：“通过数据出境安全评估的结果有效期为 2 年，自评估结果出具之日起计算。在有效期内出现以下情形之一的，数据处理者应当重新申报评估：（一）向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的，或者延长个人信息和重要数据境外保存期限的；（二）境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形、数据处理者或者境外接收方实际控制权发生变化、数据处理者与境外接收方法律文件变更等影响出境数据安全的；（三）出现影响出境数据安全的其他情形。有效期届满，需要继续开展数据出境活动的，数据处理者应当在有效期届满 60 个工作日前重新申报评估。”

〔44〕《评估办法》第 17 条规定：“国家网信部门发现已经通过评估的数据出境活动在实际处理过程中不再符合数据出境安全管理要求的，应当书面通知数据处理者终止数据出境活动。数据处理者需要继续开展数据出境活动的，应当按照要求整改，整改完成后重新申报评估。”

〔45〕 许多奇：《治理跨境数据流动的贸易规则体系构建》，载《行政法学研究》2022 年第 4 期，第 55 页。

下各成员方制定数据本地化和数据跨境流动政策的基本原则。在中国现有自由贸易协定中，RCEP 包含的电子商务条款数量最多，其电子商务章节条款内容进行了大幅扩充，一些数字贸易规则核心条款也首次包括进来，但与国际高标准规则相比仍存在不少差距。在跨境数据流动方面，RCEP 规定不强制要求计算设施本地化（第 14 条）、不得阻止通过电子方式跨境传输信息（第 15 条）等，这些条款的接受对我国来说也是一个巨大的进步，意味着我国逐步在数据安全和数据开放之间寻找平衡。相较于 RCEP 关于个人信息保护的“倡议性”规定（第 8 条），DEPA 第 4.2 条从个人信息保护法律框架关键原则的细化、非歧视性原则及信息保护公开、个人信息保护机制之间的兼容性和互操作性、数据保护信任标志等方面为个人信息数据保护提出了具体的要求。DEPA 第 4.3.2 条明确规定通过电子方式传输的信息包括个人信息，即自然人的任何信息（包括数据）都是可跨境传输的，但 RCEP 第 15 条并没有对电子传输信息是否包含个人信息作出明确界定。〔46〕 此外，RCEP 第 14 条和 DEPA 第 4.4 条及第 15.2 条（安全例外条款）都认同数据存储非强制本地化及安全例外，这事实上对目前我国国内法就数据“境内存储为原则、安全评估后出境为例外”的总基调仍存在一定的背离。

虽然中国未在跨境数据流动议题上提出具体的规则方案，且目前国内法以数据本地化存储为原则，但从中国近期申请加入 CPTPP、DEPA 来看，中国已经逐渐向数据自由流动和开放的趋势转变。欧盟 GDPR 对个人数据向第三国或国际组织传输仅限于四种方式，这给跨国公司施加了很大的个人隐私保护义务和合规成本。〔47〕 中国基于数字经济和贸易发展考虑，在未来的选择中未必会完全接受欧盟在隐私保护方面的严格要求。〔48〕 我国目前不仅在跨境数据流动的部分法律法规中存在规则模糊等问题，而且个人信息和部分商业场景的重要数据出境评估规定缺乏灵活性，数据的分级和分类管理目前并没有成熟的制度安排。这些问题势必会影响中国参与经济全球化、拓展全球数字服务市场的进程。

从国际贸易规则的角度来看，“一般例外”条款可以作为平衡数字主权和数据自由流动的有力工具。DEPA 将 GATS 第 14 条纳入一般例外情况，即授权成员国为了满足合法公共政策目标或保障基本安全利益而采取不符合规定的措施。〔49〕 这样来看，根据 DEPA“美式规则”特点，成员国在原则上应当鼓励数据的跨境自由流动，但这种自由并非绝对，其受到例外条款对安全、隐私等方面的限制。这考虑到更多缔约方的自身诉求，给予缔约方更大的数据流动管制空间，〔50〕 为我国数据出境评估体系与 DEPA 的“接合”性提供了解释的依据。问题在于，如何对第 14 条（c）（iii）项下的“安全”进行解释。〔51〕 这涉及何种安全利益可以纳入 GATS 例外条款中。尤其是近年来，

〔46〕 参见周念利、于美月：《中国应如何对接 DEPA——基于 DEPA 与 RCEP 对比的视角》，载《理论学刊》2022 年第 2 期。

〔47〕 这四种被允许的数据跨境传输方式分别是：数据控制者和处理者基于充分性决定、提供适当保障措施、建立有约束力的公司规则、特殊情况下的例外。参见戴龙：《论数字贸易背景下的个人隐私权保护》，载《当代法学》2020 年第 1 期。

〔48〕 参见前引〔47〕，戴龙文。

〔49〕 See DEPA Article 15.1&15.2.

〔50〕 参见前引〔26〕，陈寰琦、陆锐盈文。

〔51〕 参见田翔宇：《我国跨境数据流动监管体系的国际法分析——以 GATS“一般例外”条款为视角》，载《人民法治》2018 年第 24 期。

国家安全范畴从传统安全扩展到非传统安全，如何构成威胁国家安全的条件几乎完全由一个主权国家自己决定。国家安全审查制度等国内法上的规则和制度不断外溢，成为一种国际通行的做法和监管工具，国家安全呈现概念泛化且考量因素模糊等特点。在此背景下，以“特朗普政府打压TikTok”为代表的、以维护国家安全为由限制跨境数字交易、投资和数据访问的事件频频出现，削弱了国际规则体系，侵蚀了全球化发展的法律基础、国际机制和法治逻辑。〔52〕DEPA目前也没有对这些措施的合理限制作出更为具体的国家安全例外规定。中国可以申请加入DEPA为契机，与其他成员国探讨例外条款在数据流动方面的包容性，探寻以维护数据主权为前提的数据流动和数据安全之间的最佳平衡点。

近年来中国的崛起已对美国引领的西方主导地位带来潜在挑战，视中国为“战略竞争对手”已成为美国两党的战略共识，中美在数字领域的竞争将会更加激烈。美国主导构建的“印度—太平洋经济框架”（The Indo-Pacific Economic Framework，IPEF）包含建立一个新的数字治理框架以管理印太地区的数字经济和跨境数据流动。〔53〕目前参与IPEF框架的13个初始国家包括了韩国、新西兰以及文莱、印度尼西亚、马来西亚、菲律宾、新加坡、泰国、越南七个东盟国家。结合数字经济协定签署的集中地、数字税等数字规则的覆盖地以及后疫情时代经济复苏的进展与规模看，印太地区是全球数字博弈的重点区域。〔54〕中国处于印太地区数字供应链的中心，美国印太战略的构建和实施可以视为对中国“数字丝绸之路”和“一带一路”的制衡，以削弱中国在印太地区日益增长的影响力。在此背景下，构建符合中国国情、与世界接轨的跨境数据流动体系就尤为重要和紧迫。中国申请加入DEPA，体现了我国对数字经济国际合作的高度兴趣与构建全球数字经济框架的最新努力。DEPA为不同国家之间的企业合作提供了技术和规则交流的有利平台，中国应当借助申请加入DEPA的契机，积极参与全球数字产业链供应链治理，探索数据驱动创新体系和安全发展模式，在维护我国网络安全的基础上稳健地开放数字市场，引领全球产业链的发展和数字贸易规则的构建。

四、结　语

随着数字经济的迅速发展，数据已成为未来改变全球竞争格局、重塑全球经济结构、重组全球要素的重要资源。越来越多的国家将数字治理和跨境数据流动规则作为其双边和区域贸易协定的要素和章节。中国申请加入DEPA，意味着中国继加入RCEP后，进一步接受DEPA更高水平的数字治理理念和规则，将与DEPA缔约国共同参与全球数字治理，并展开进一步的合作和交流。这既是中国参与全球数字治理的一次机遇，又在对标国内规则、平衡数据安全和开放流动难题、中美战略竞争等诸多方面面临挑战。虽然我国正在逐步构建数据出境评估体系，但从主要内容上来看仍然与DEPA等高水平数字经济规则存在一定的张力。中国应当综合评估DEPA的协

〔52〕 参见沈伟：《驯服全球化的药方是否适合逆全球化?》，载《人民论坛·学术前沿》2020年第12期。

〔53〕 See the White House website，FACT SHEET：Indo-Pacific Strategy of the United States，available at https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf，last visited on Feb.12，2022.

〔54〕 参见翟崑：《数字全球化的战略博弈态势及中国应对》，载《人民论坛》2021年第17期。

定内容，结合目前国内数字经济发展状况，有选择地参加 DEPA 并提出数据治理的“中国方案”，与其他国家在尊重主权的基础上共同构建全球数字治理新格局。

Abstract：With the development of digital technology，data has become a fundamental and strategic resource for most of the countries. The competition for data resources among countries has become increasingly intense. The issues such as cross-border data flow have become the focus of international attention. Since data has the attributes of both property and personality interests，there are differences in the philosophy of data governance among countries. At present，the global data governance framework has not yet been formed. The Digital Economy Partnership Agreement (DEPA) is the first special agreement for the digital economy in the world. In terms of data issues，it mainly draws on American digital rules and adopts a flexible modular framework. It also reflects the demands of small and medium-sized countries such as Singapore in terms of digital governance. Compared with traditional comprehensive trade agreements，it is more contemporary，flexible and extensible. From the perspective of the data exit assessment system being constructed in China，there is a tension between China's domestic digital rules and high-level international digital rules such as DEPA. China's application to join DEPA is conducive to promoting the development of its own digital economy and international cooperation，improving the level of data governance，and further expanding China's voice in global data governance.

Key Words：DEPA，digital economy，global data governance

（责任编辑：肖　芳　赵建蕊）

财经法学 No. 2，2021
pp. 79 - 97

虚拟货币的国际监管：以反洗钱为起点走出自发秩序

吴　云　朱　玮*

内容提要：虚拟货币诞生已逾十年，其并未对现有法定货币体系造成冲击，因此，主要国家货币当局并未对个人持有并使用虚拟货币进行禁止。同时，由于虚拟货币是否适合普通投资者并没有定论，主要国家证券监管当局也并未正面注册或审批任何一种面向公众投资者发行的虚拟货币或与其挂钩的金融产品。但是，投机、欺诈和严重的洗钱问题促使各国当局不得不以实质性手段回应关切，在金融行动特别工作组（FATF）推动下，2019 年各国当局首先就虚拟货币反洗钱监管达成了共识，全球范围内的虚拟货币的监管框架正式形成，从根本上改变了行业自发生态。但反洗钱监管规则仅限于区块链外部活动时的洗钱预防问题，虚拟货币的链上治理将是下一个阶段监管的核心问题，也是挑战性最大的问题。

关键词：虚拟货币　反洗钱监管　区块链治理

一、引论：背景、主要作品回顾和本文的贡献

2009 年 1 月，中本聪设计的比特币（bitcoin）诞生，标志着虚拟货币作为一种现象级事件正式登上了历史舞台。中本聪设计比特币的目的在于创造一种点对点的支付系统，这个系统不依赖于任何第三方信任，使比特币成为一种开源的、基于网络的、点对点的匿名电子货币。〔1〕比特币

* 吴云，中国人民银行反洗钱局制度处副处长，金融风险分析师（FRM）；朱玮，北京无知智慧人工智能科技有限责任公司区块链工程师。

衷心感谢中国人民银行反洗钱局的领导和同事给予笔者在相关课题中的研究和参与机会。本文为作者个人学术思考，不代表所在机构观点。

〔1〕 See Satoshi Nakamoto，Bitcoin：A Peer-to-Peer Electronic Cash System 1，8（2008），available at https://bitcoin.org/bitcoin.pdf，last visited on Jun. 10，2020.

很大程度上受哈耶克私人货币思想的影响，从一开始就怀有实践私人货币实验的宏大理想。〔2〕但哈耶克所挑战的是国家对货币发行的垄断权力。〔3〕中本聪所挑战的是传统社会对第三方的信任，包括哈耶克所支持的商业银行，哪怕这些商业银行是在充分竞争的市场中。哈耶克要解决的问题是政治和经济问题，即如何实现货币的市场化和自由竞争；而中本聪要解决的问题是技术问题，即如何让虚拟货币摆脱对第三方可信服务器的依赖（即对中心化服务器的依赖）。〔4〕因此，比特币的创新不仅体现在技术层面，也体现在社群生态的设计上，开启了用区块链技术实现“去中心化”的生态治理模式，一切都是自发的，无需一个中心节点的组织、管理和裁决。

“虚拟货币”一词随着比特币的产生而有了新的内涵。在比特币产生之前，“虚拟货币”仅指在特定网络世界使用的代币，典型例子是游戏币；而比特币则可以实现广泛的交易和兑换功能，可在一定程度上承担货币的职能。为区分这两种情况，国际组织和主要监管当局将前者称为“不可转换式”（non-convertible）或“封闭式”（closed）虚拟货币，将后者称为“可转换式”（convertible）或“开放式”（open）虚拟货币。不可转换式虚拟货币被设定为特定社群内的单项用途，典型的如“Q 币”，持有者仅能在腾讯游戏世界使用，不能转移交付给第三方，是特定用途的电子化商品。可转换式虚拟货币可在不同用户之间转移，可以实现与法定货币、其他虚拟货币的双向兑换。〔5〕本文所讨论的虚拟货币仅指可转换式虚拟货币。

我们承认，虚拟货币这一场私人货币实验运动中，诞生了一系列影响经济模式和社会格局的技术创新，这些技术创新一般被总称为“区块链技术”，在价值流转、权利证明、商业模式等方面都有广泛的运用空间。〔6〕但是，从货币职能的角度，这场私人自发运动并不成功，反而产生了巨大的负面效果。徐忠和邹传伟指出了比特币的支付容量过小成为制约其作为支付手段的瓶颈，但限于主题需要并未展开进行详细论证和说明。〔7〕吴云和朱玮结合技术分析，从货币职能的角度，全面分析了虚拟货币的社会实验是一场失败的运动，指出内在技术缺陷导致其无法成为公众广泛使用的交易媒介，在无监管状态下比特币价格被严重操纵，不仅未能展示普惠金融的优势，相反，比特币的匿名性和跨国性被犯罪活动滥用为洗钱工具。〔8〕

〔2〕 关于哈耶克思想对虚拟货币的影响，可参见 Luca Fantacci，Cryptocurrencies and the Denationalization of Money，48 (2) *Int'l J. Pol. Economy*，105，105－112 (2019).

〔3〕 哈耶克认为政府并不值得相信，历史一再证明政府如果垄断某种商品一定会导致无效率，政府发行货币的历史，无一不以政府失信、货币贬值终结。私人货币发行者之间的竞争要优于政府的垄断。（See F. A. Hayek，*Denationalization of Money*：*The Argument Refined* ，Hobart Paper，1978，p. 9.）

〔4〕 参见朱玮、吴云、杨波：《区块链简史》，中国金融出版社 2020 年版，第 3 页。

〔5〕 欧洲中央银行较早提出了通过“可转换性”对虚拟货币进行监管分类，并提出只有可转换式虚拟货币才具有金融监管意义。这种分类方法被国际监管界和主要国家监管当局所普遍接受。[See European Central Bank，Virtual Currency Schemes，p. 5 (October 2012).] 另可参见〔德〕伦纳·库尔姆斯：《比特币：自我监管与强制法律之间的数字货币》，廖凡、魏娜译，载《国际法研究》2015 年第 4 期。这是中文作品中少有的深入讨论虚拟货币可转换性的可信佳作。

〔6〕 参见前引〔4〕，朱玮、吴云、杨波书，第 179－226 页。

〔7〕 参见徐忠、邹传伟：《区块链能做什么、不能做什么?》，载《金融研究》2018 年第 11 期。该文在论述虚拟货币的社科类文章中堪称技术严谨的典范。

〔8〕 参见吴云、朱玮：《虚拟货币：一场失败的私人货币社会实验?》，载《金融监管研究》2020 年第 6 期。

沃巴赫的《信任，但需要验证：论区块链为何需要法律》〔9〕是跨学科的佳作，其法律论证建立在技术的真实背景之上。该文从区块链治理的角度分析监管的必要性，而本文则是立足虚拟货币的职能和社会效果来分析监管的必要性，两者角度不同，可以相互补充和验证。在具体的论证上，两者也可以相互补充验证。例如，沃巴赫文指出信任区块链的分布式记账技术“不可与信任特定个人和机构混为一谈”，而本文关于虚拟货币价格操纵的论述则是对这个判断的恰当注解。

中外学者虽然对虚拟货币是否构成“货币”有所争议，但至少都肯定其可以或者部分可以执行货币的三大职能（交易媒介、价值储藏、计价单位）。〔10〕2017 年以来，随着“代币首次发行”（ICO）在中国监管文件中出现，〔11〕一些学者援引美国等法例，论证虚拟货币属于证券。〔12〕一些文献也开始跟踪国际反洗钱规则的变化，并梳理了虚拟货币的国际反洗钱监管动态。〔13〕

但是，有些文献在论证某种属性时，往往带着非此即彼的基本假设，在论证一种性质时会否定另外一种性质。例如，杨东提出虚拟货币的性质是众筹〔14〕（美国法上可以豁免监管的一类证券），杨延超认为虚拟货币应该属于“货币”〔15〕。这些作品的共同不足在于，试图论证出“唯一”的属性，忽视了从金融监管的角度看，虚拟货币可以同时具有多重属性。

在国内文献中，综合视角的尝试不多，仅见孙国峰和陈实的短评文章从综合的视角分析了美国对虚拟货币的多重监管，〔16〕朱玮、吴云和杨波初步提出了“虚拟货币三重属性”，即货币（或者执行货币职能）、证券和价值转移手段（反洗钱的监管对象）〔17〕。多重监管是很常见的现象，以中国证券行业为例，证监会作为行业主管部门要对证券机构（准入、内部治理等）和证券行为（发行、交易等）实施监管，中国人民银行作为反洗钱主管机关实施监管。

本文分析了虚拟货币三个金融属性的监管框架，并结合工作经验对监管框架内在逻辑进行了分析；回答了为什么国际上首先就虚拟货币反洗钱问题形成了成熟的监管规则和共识，而证券监管和货币监管尚处在起步阶段；同时，对虚拟货币反洗钱监管及其对整个金融监管框架的影响进行了分析。

---

〔9〕 参见〔美〕凯文·沃巴赫：《信任，但需要验证：论区块链为何需要法律》，林少伟译，载《东方法学》2018 年第 4 期。

〔10〕 例如，贾丽平：《比特币的理论、实践与影响》，载《国际金融研究》2013 年 12 期。该文认为，虽然虚拟货币还没有成为真正的货币，但可以执行货币的职能。该文是国内较早就虚拟货币的货币性质进行研究的论文，论证比较中肯，结论也广为接受。

〔11〕 2017 年，中国人民银行等七部委颁布了《防范代币发行融资风险的公告》，这是官方对外规范性文件中第一次出现“代币首次发行”。

〔12〕 例如，孙国峰、陈实：《论 ICO 的证券属性与法律规制》，载《管理世界》2019 年第 12 期。该文比较娴熟地运用美国证券监管规则分析了虚拟货币的证券属性。

〔13〕 参见蔡制宏：《数字货币发展状况、可能影响及监管进展》，载《金融发展评论》2015 年第 3 期。

〔14〕 参见杨东：《“共票”：区块链治理新维度》，载《东方法学》2019 年第 3 期。

〔15〕 参见杨延超：《论数字货币的法律属性》，载《中国社会科学》2020 年第 1 期。该文提出了“数字货币新货币说”，但从其表述来看，应仅限于“虚拟货币”（私人发行的数字货币）中的加密货币（非中心化、分布式的虚拟货币）。

〔16〕 参见孙国峰、陈实：《美国虚拟货币监管借鉴》，载《中国金融》2017 年第 19 期。该文虽然仅是一篇非学术的简短评论，但比较全面讲解了美国对虚拟货币的金融监管框架，是国内文献中少有的多维度讲解虚拟货币的文章。但限于篇幅和期刊性质，该文仅讲解了监管框架，尚未深入分析虚拟货币的性质。

〔17〕 参见前引〔4〕，朱玮、吴云、杨波书，第 271－283 页。

尤其值得注意的是，反洗钱监管在国际上早已是“大热门”，但在中国尚属“偏门”，《反洗钱法》通过仅 15 年时间，法学界研究还多限于刑法学界，罕有真正从“金融监管”角度进行的研究。〔18〕学界很多作品强调虚拟货币的洗钱风险，但罕有专业性分析（内在洗钱风险等）。

本文在这些方面填补了空白。本文的基本逻辑是：虚拟货币作为一场货币实验的失败反证了国家干涉的必要性；由于虚拟货币并未对现今货币体系形成冲击，且虚拟货币是否适合普通投资者参与也存在很大争议，而虚拟货币价格操纵、通过虚拟货币洗钱则是现实紧迫的问题，因此，各国首先就虚拟货币反洗钱监管达成了共识，迈出了虚拟货币监管的关键性一步。

本文的主要贡献在于：按照虚拟货币三重属性的观点，提出虚拟货币监管的框架和内在逻辑，对强制性国际反洗钱标准及其影响进行分析，并就如何对区块链治理实施监管这样深层次的问题进行了展望。

二、虚拟货币的失败：监管的必要性前提

虽然学界对“什么是货币”有多种学术观点，〔19〕但是，对于货币的职能却有高度共识，即货币具有价值储藏、交易媒介和计价单位三大职能〔20〕。同理，对虚拟货币是否构成“货币”争论很多，〔21〕但是，虚拟货币已经可以执行货币职能已经是不争的事实〔22〕。吴云、朱玮曾指出，在虚拟货币这一场私人货币实验运动中，虽然诞生了一系列影响经济模式和社会格局的技术创新，在价值流转、权利证明、商业模式等方面都有广泛的运用空间，但是，从货币职能的角度，这场私人自发运动并不成功，而且产生了巨大的负面效果。〔23〕总结起来，主要有以下几个方面：

（一）虚拟货币执行货币职能存在根本缺陷：以比特币为例

法定货币与比特币的对比可参见表 1，以下分别详细阐述。

---

〔18〕 我国 2006 年通过的《反洗钱法》是参照国际标准制定的金融监管性法律，其基本逻辑是通过对金融机构等义务机构实施监管构筑反洗钱预防体系，而如何惩治洗钱行为则由《刑法》规定。“洗钱”是一个不断发展的概念。本文对“洗钱”采用广义的概念，“洗钱”包括“狭义的洗钱”“恐怖融资”两个方面。“洗钱”在更广义的情况下还包括 FATF 框架下的“扩散融资”，指的是向联合国安理会所制裁的朝鲜、伊朗个人或实体提供资金、资产或与其进行交易的行为。

〔19〕 例如，商品货币学派认为货币是商品中衍生出的一般等价物，信用货币学派认为货币仅是计量“信用—债务”关系的会计工具。(See Thomas H. Greco, JR., *Money: Understanding and Creating Alternatives to Legal Tender*, Chelsea Green Publishing, 2001, p. 22.)

〔20〕 这是中外主流教科书中对货币基本功能的界定。例如，N. Gregory Mankiw, *Principles of Economics*, Cengage Learning, 2018, p. 605；逄锦聚等主编：《政治经济学》，高等教育出版社 2014 年版，第 50－52 页。该《政治经济学》教科书中还列举了延期支付（书中称为“支付手段”）和世界货币两个职能，延期支付职能可被认为是交易媒介职能的延伸，两者具有包含关系，世界货币职能是前几个货币职能的国际化延伸。

〔21〕 王信、骆雄武提出货币从民间到官方是一个历史趋势，虚拟货币由于缺乏国家信用支撑，很难获得认可，并且进一步提出央行数字货币的推出将在吸收虚拟货币技术优势的基础上进一步强化国家法定货币的地位。(参见王信、骆雄武：《数字时代货币竞争的研判及应对》，载《国际经济评论》，2020 年第 2 期，第 25－35 页。) 本文赞同该文的论证和观点，并进一步认为，应当从正当性和功能两个角度来理解虚拟货币的货币属性，而且要考虑获到社会共识是一个动态和演化的过程。

〔22〕 See Mark Carney, The Future of Money, Speech by the Governor of the Bank of England to the inaugural Scottish Economics Conference , Edinburgh University (March 2, 2018). 该演讲很大程度上代表了国际金融监管界的共识。国内学术文献可参见前引〔10〕，贾丽平文。

〔23〕 参见前引〔8〕，吴云、朱玮文。

表 1　　**法定货币和比特币的对比**

	法定货币	比特币	后果
系统容量	现有电子支付系统理论上可以无限扩容	系统容量有理论上限	比特币无法成为公众大规模使用的支付手段
支付速度	几秒（现有电子支付）	平均 10 分钟	
币值波动率	相对稳定（主要货币）	超过主要货币 10 倍	比特币无法成为价值储藏手段和可信计价单位
支付成本	中国国内银行转账：0 中国国际电汇：200～300 元	0.58～224 元 （2017 年）	比特币并未展现普惠金融的优势
技术安全性	高	低	

1. 系统承载容量有限无法用于大规模支付

比特币特殊的技术安排导致其交易容量有限，不能承载社会大规模使用。比特币的技术设计限定了平均每秒 7 笔的交易容量，而支付宝可承载的峰值交易记录是每秒 25.6 万笔（2017 年 11 月 11 日）。截至 2019 年 11 月 23 日，比特币共有约 60.5 万个区块，理论上目前的比特币系统仅能承载约 24.78 亿笔交易，不及中国第三方支付的三天清算量。相反，现有的中心化电子支付系统（银行电子支付系统、第三方支付系统）可以通过系统的软硬件升级做到无限扩大容量。

尽管后续的虚拟货币试图对比特币进行改进，但技术缺陷仍未有根本突破。例如，根据以太坊白皮书推算，以太币（ETH）的理论最高承载量仅为每秒 15 笔交易。柚子币（EOS）声称每秒承载容量可达到 3996 笔交易，〔24〕这一容量使其至多作为小的国家、地区或者行业的支付方式。最近提出的“闪电网络”寄希望于通过离线技术（以比特币作为“抵押”在闪电网络进行交易，通过比特币系统作最后“结算”）实现比特币无延迟、低成本交易，但目前仅有 895 个比特币的支付容量，〔25〕且存在一系列技术性不足〔26〕。

2. 交易速度极慢导致虚拟货币无法用于日常支付

从单笔处理速度看，比特币比现有普遍使用的电子支付方式落后了几个数量级，无法用于公众日常使用。实践中比特币每笔交易的平均确认时间为 10 分钟（大额交易需要的确认时间更长），相反，支付宝每笔交易时间为 3 秒，而常用的非接触卡交易时间少于 1 秒。2017 年 12 月，比特币价格上涨导致比特币交易暴增，比特币系统开始拥堵，当月一笔交易平均等待时间是 2 天 2 夜。〔27〕

因此，从交易媒介的角度，比特币及后续出现的多种虚拟货币由于容量过小、交易速度过慢，无法作为公众大规模使用的支付手段，只能用于对时限要求不高的大宗交易。

〔24〕 参见其官方网站，载 https://eosnetworkmonitor.io/，最后访问时间：2020 年 3 月 6 日。

〔25〕 2018 年 1 月闪电网络系统在比特币主网上线，目前闪电网络有节点 11624 个，支付通道 36289 个，整体支付容量为 895 个比特币。数据来源于 1ml 网站，载 https://1ml.com/statistics，最后访问时间：2020 年 3 月 6 日。

〔26〕 如闪电网络结构趋向中心化，网络运行效率依赖大型中心节点的支付容量，而非点对点网络的规模扩张。

〔27〕 数据来源：https://www.blockchain.com/charts，最后访问时间：2020 年 3 月 6 日。

3. 币值波动过大导致虚拟货币不能承担价值储藏手段和计价单位职能

比特币在其发展初期的 2011 年曾经在两个月内价格从 0. 75 美元上涨 40 倍，达到 30 美元，随之 2012 年 2 月跌破 2 美元，跌幅超过 93%。最近一次较大波动发生在 2019 年 11 月 21 日，24 小时内比特币价格下跌 7%。〔28〕 相反，主要国家货币日涨跌幅达到 1%、主要股票指数的日涨跌幅达到 2%～3%已经属于较大价格波动。

吴云和朱玮通过统计长期以来不同资产价格变化率发现，比特币的波动率是主要货币波动率的 10 倍，是贵金属波动率的 3～5 倍，是股票市场波动率的 3～5 倍，是原油波动率的 3 倍。〔29〕比特币极高的波动率超过了现有主要货币波动率一个数量级，远高于主要风险资产的波动率，无法成为价值储藏的手段，交易各方无法约定比特币计价的未来商品和服务。

因此，从货币职能角度看，由于交易媒介和价值储藏两个核心职能存在缺陷，以虚拟货币标价（计价单位）的体系难以稳定和有效，虚拟货币难以成为可信的计价单位。

4. 容量有限、速度慢导致交易费用过高

比特币的支持者一再宣扬：对于无法从现有金融体系中获得服务的人们（如偏远地区没有银行网点，民众难以获得金融服务），虚拟货币的去中心化可以增强金融的包容性。然而，这仅仅是一种理论上的推演，完全不符合实际情况。虚拟货币虽然可以脱离金融中介在点对点网络中流转，但是，这种虚拟货币的流转需要消耗系统算力，用户支付转账时必须要给提供算力的矿机支付一定比例的虚拟货币以补偿其提供的算力。〔30〕

当用户转移比特币时，首先要在钱包上构造交易，然后提出一个手续费报价，交易广播出去到达矿机后，矿机一般会按照手续费由高到低进行“接单”，形成一个众多钱包各自分散报价和众多矿机自主选择交易的撮合体系。也就是说，比特币的交易费用由用户和矿机间的自由市场所确定，并无固定比例和规则约束。随着虚拟货币币值的升高和交易活跃程度增加，转账手续费也会越来越高。其中，虚拟货币币值升高，意味着等量手续费对法定货币的相对价格上升；交易活跃程度增加，则大量交易在矿机中形成基于手续费高低的竞争。用户若希望矿机更早验证和打包自己的交易，则需要支付更高的手续费。

2016 年每笔比特币交易费折合人民币平均为 0. 58 元，2017 年 12 月由于交易拥堵和比特币价格暴涨则高达 224 元。〔31〕 相比而言，我国内银行国内网络转账已经实现零手续费，几大银行对境外汇款每笔手续费一般在 200～300 元之间，比特币转账在成本上并无任何优势。

5. 安全性较差

比特币私钥一旦丢失将无法追回。〔32〕 例如，2013 年虚拟货币交易所 Mt. Gox 价值 4. 5 亿美

〔28〕 关于比特币的历史价格来源：http://www. blockchain. com/charts，最后访问时间：2020 年 3 月 6 日。

〔29〕 参见前引〔8〕，吴云、朱玮文。

〔30〕 矿机为系统提供算力可以获得两部分利润，一是系统提供挖矿收益，二是用户提供的转账手续费。按照比特币的算法设计，2140 年之后，比特币总量不再增加，矿机的收益将只有用户的转账手续费。（参见前引〔4〕，朱玮、吴云、杨波书，第 86 页。）

〔31〕 数据来源：https://www.blockchain.com/charts，最后访问时间：2020 年 3 月 6 日。

〔32〕 See Christian Beer，Beat Weber，Bitcoin-The Promise and Limits of Private Innovation in Monetary and Payment Systems，Q4 *Monetary Pol'y and the Economy*，53，53－66 (2015).

元比特币丢失，2016 年虚拟货币交易所 Bitfinex 价值 7000 万美元的比特币丢失。虚拟货币对使用者的技术水平提出了很高的要求，往往超出了普通人的技术能力。相反，现有的电子支付体系经过反复调试已经兼具较高的安全性和便捷性。

这也提出了普惠金融的悖论：若使用者能够安全使用虚拟货币进行支付，那么他一定拥有电子设备和相应的技术能力，可这样的人往往有充分的渠道获得现有金融体系的服务。

（二）比特币价格被人为操纵，刺激了虚拟货币泡沫

信任区块链的分布式记账技术不可与信任特定个人和机构混为一谈。〔33〕一些大交易所利用独特地位操纵虚拟货币价格。

第一次是 2013 年 10 月 3 日至 11 月 30 日，每枚比特币的价格由 116 美元涨至 1150 美元，两个月内暴涨 10 倍。一则学术研究用严谨的数据和逻辑证明，当时全球最大的交易平台 Mt. Gox（注册地在日本）虚增几个特定账户中的美元资金和比特币，然后通过几个账户之间的交易人为拉高比特币价格。〔34〕2019 年 3 月，东京地方法院判决 Mt. Gox 的 CEO 篡改记录虚增资产罪名成立。〔35〕

第二次是 2017 年 3 月 27 日至 12 月 17 日，每枚比特币价格由 1046 美元上涨至日间最高 20089 美元，九个月之内暴涨 20 倍。一则学术研究揭露，Tether 公司通过发行没有实际支持资产的稳定币 USDT 在其旗下的 Bitfinex 交易所操纵比特币价格。〔36〕由于该研究的巨大影响力，2018 年 11 月美国司法部和美国期货交易委员会（CFTC）联合对比特币背后可能存在的价格操纵进行了调查。〔37〕

比特币价格的暴涨，引起了对虚拟货币投资的跟风效应，刺激了“山寨币”的大量出现，代币首次发行（ICO）变成了热门话题，各种“币”价格暴涨。

早期的山寨币运营，需要一定的技术和成本投入，如早期的万事达币（Mastercoin）就是比特币二层协议的经典。2015 年以太坊的出现彻底消除了山寨币的技术门槛。以太坊的智能合约使用 Solidity 语言，开发者可以极为便捷地使用 Solidity 开发出新的虚拟货币，只需部署一个标

〔33〕 参见前引〔9〕，凯文·沃巴赫文。

〔34〕 See Neil Gandal et al.，Price Manipulation in the Bitcoin Ecosystem，95 *J. Monetary Econ.*，86，86－96（2018）.

〔35〕 有关案件的情况参见 Yuki Furukawa，Former Mt. Gox CEO Mark Karpeles Gets Suspended Jail Term，March 15，2019，载 https：//www. bloomberg. com/news/articles/2019－03－15/former-bitcoin-baron-mark-karpeles-gets-suspended-jail-term，最后访问时间：2020 年 6 月 10 日。

〔36〕 See John M. Griffin，Amin Shams，Is bitcoin really un-tethered? October 28，2019，available at SSRN：https：//ssrn.com/abstract＝3195066，last visited on Jun. 10，2020. 此论文更新版本将发表于权威期刊《金融学期刊》（The Journal of Finance）。作者通过对 200G 的交易数据的研究，证明了几个主要假设：（1）当比特币价格下跌时，大量 USDT 被用来购买比特币；（2）当比特币价格在整数关口附近时，大量 USDT 被用来购买比特币；（3）存在明显的“月底效应”。每个月月底会计师事务所要审计 USDT 在该时点是否有充足的美元作为支持资产，审计前存在明显的卖出比特币换回 USDT 的情况，这在一定程度上验证了 Tether 所发行的 USDT 并没有足额支持资产的传闻。在更新的版本中，作者增加了一个新的发现，一个账户的交易者展现了“未卜先知”（clairvoyant）的把握交易时点的能力，对比特币价格施加了“极端大的”（extremely large）影响力。

〔37〕 See Matt Robinson，Tom Schoenberg，Bitcoin-Rigging Criminal Probe Focused on Tie to Tether，Bloomberg，November 20，2018，at Markets；Kate Rooney，As Bitcoin Nosedives，Regulators Said to be Investigating Whether It Was Propped Up Illegally，CNBC，November 20，2018，available at https：//www. cnbc. com/2018/11/20/regulators-investigate-whether-bitcoin-price-was-propped-up-illegally. html，last visited on Jun. 10，2020.

准的 ERC20 代码即可完成，其简易程度如同注册一个域名，用时不超过 10 分钟。据 etherscan.io 网站的统计，在 2018 年 6 月 12 日以太坊上的 ERC 20 代币智能合约共计 90738 种，到 2020 年 3 月 5 日已经增加到 245504 种。其中真正有技术含量或价值的，凤毛麟角。

根据 Coinmarketcap 按照市值排名对 5164 种虚拟货币的回溯性统计，2014 年 1 月 1 日，虚拟货币市场总市值为 106 亿美元（其中比特币 94 亿美元），而到了 2017 年 12 月 17 日，虚拟货币总市值为 8003 亿美元（其中比特币 3200 亿美元）。比特币在虚拟货币市值中的比重由约 90% 降为约 40%，虚拟货币领域由比特币一枝独大变成了遍地开花。

从 2013 年起，美国证券交易委员会（SEC）通过风险提示公布了大量以虚拟货币为幌子的欺诈案例。〔38〕在中国，大量山寨币沦为空气币，完全成为投机和诈骗的工具。如“太空链”诈骗金额高达 10 亿元；〔39〕“GGP 共赢积分”以虚拟货币为噱头进行传销，涉案金额 10 亿元；〔40〕“PlusToken”席卷全球 170 个国家，涉及受害人 300 万，涉案金额 200 亿元〔41〕。

（三）被洗钱和犯罪滥用

虚拟货币由于其匿名性、无国界性，具有被洗钱利用的很高内在风险（inherent risk），容易被洗钱和犯罪活动所利用。〔42〕几乎所有的“暗网”市场都通过虚拟货币进行交易。至少一半左右的暗网活动是违法犯罪活动。〔43〕暗网也被恐怖主义活动利用，伊斯兰国（ISIS）曾经广泛使用暗网进行信息分享、招募、宣传，并通过虚拟货币筹集资金。〔44〕

虚拟货币也出现在各类网络犯罪活动中，越来越多的犯罪活动不再通过传统的金融系统进行支付，而是通过虚拟货币收取勒索的赎金等，从而逃避监管和执法机关的追踪。〔45〕

虚拟货币至少一半用于违法犯罪活动。根据 2018 年的研究推算，四分之一的比特币用户、二分之一的比特币交易与非法活动有关，2015 年至 2017 年每年大约有 720 亿美元的规模，相

〔38〕 例如，SEC，Investor Alert：Ponzi Schemes Using Virtual Currencies（July 23，2013）；再比如 SEC，Investor Alert：Bitcoin and Other Virtual Currency-Related Investments（May 7，2014）。

〔39〕 参见冯樱子、金微：《太空链破发 90% 大佬纷纷撇清关系》，载《华夏时报》2018 年 4 月 9 日，第 13 版。

〔40〕 2019 年该案已经二审宣判，并被最高人民检察院列为 2019 年典型案例。（参见最高人民检察院官方网站，载 https://www.spp.gov.cn/xwfbh/wsfbh/201912/t20191203_440338.shtml，最后访问时间：2020 年 3 月 6 日。）

〔41〕 关于 PlusToken 的相关报道参见毕丹丹：《警惕“虚拟货币”“区块链”骗局：勿让非法集资钻空子》，载《上海金融报》2019 年 11 月 8 日，第 10 版；《涉案 200 亿 币圈最大的资金盘崩了》，载《知识经济》2019 年第 20 期。

〔42〕 内在风险（inherent risk），也译为“固有风险”，是反洗钱专业术语，指在不考虑任何风险控制措施的情况下所暴露的洗钱风险。例如，在我国，由于股票采取公开集中竞价交易，在没有任何控制措施的情况下，股票交易比银行转账交易的洗钱风险要低，可以认为前者比后者的洗钱内在风险更低。[See The Wolfsberg Group，Wolfsberg FAQs on Risk Assessments for ML，Sanctions and Bribery & Corruption，p. 7（2015）.]

〔43〕 See Gollnick，Clare，Emily Wilson，*Separating Fact from Fiction*：*The Truth about the Dark Web*，Terbium Labs，2016，pp. 5－6.

〔44〕 万维网（the World Wide Web）分为“表层网”（surface web）和“深网”（deep web）两个部分。我们日常能够使用的仅是表层网，能够通过搜索引擎索引，可以通过普通浏览器直接登录；不能被搜索引擎索引的被称为“深网”，也叫“不可见网”（invisible web），日常常见的包括电子邮件、网络银行、付费数据库、公司的内网等。根据估计，“深网”的规模至少是“表层网”的 4000～5000 倍。“暗网”（dark net，dark web）是“深网”的一部分，通过加密技术刻意将内容、网址等隐藏起来，需要通过特殊的软件、授权或设置才可以接入。（See Kristin Finklea，Dark Web 2－3，9－12，Congressional Research Service：R44101，2017.）

〔45〕 See ECC Europol，The Internet Organised Crime Threat Assessment（IOCTA）2015 at 11（Sept. 30，2015）.

当于美国和欧洲每年毒品犯罪额的总和。〔46〕无论是相对数量还是绝对数量都是非常惊人的。〔47〕

三、为什么虚拟货币监管从反洗钱开始

虚拟货币严重的价格操纵、投机以及被洗钱和犯罪滥用风险，反证了国家对货币秩序进行干涉的必要性。但国家对虚拟货币不同维度干涉的急迫性和必要性是不同的。

由于虚拟货币对法定货币体系的冲击并未显现，衍生出的审慎问题也尚在讨论之中，因此，货币相关当局对虚拟货币基本处于观察之中。同时，由于投资者适当性问题的困扰，美国等主要国家尚未允许任何一种虚拟货币对公众发行，国际社会也没有就如何向普通投资者发行虚拟货币形成大范围的共识，注册或审批的正面案例不多。相反，目前在投资领域虚拟货币暴露的更多是价格操纵、欺诈等问题，因此，主要国家对虚拟货币的监管以采取行政处罚、司法调查等方式为主。同时，由于通过虚拟货币洗钱的问题日益严重，各国反洗钱当局已经共同认识到监管虚拟货币的现实必要性和急迫性。

（一）金融监管的基本框架和问题

传统的金融监管包括审慎监管和行为监管两个目标。审慎监管包括宏观审慎监管和微观审慎监管。前者的目的是维持金融体系的稳定，一般由作为货币当局的中央银行负责；后者的目标是单个金融机构的稳健性，由中央银行或者单独的审慎监管机构负责。行为监管以金融消费者保护为目的创造并维护金融市场秩序的公平性、透明性（如证券市场的强制信息披露）。在现有的法定货币体系中，由于货币会通过金融中介（典型的是商业银行）进行信用放大，进而衍生出审慎监管问题，为简化讨论，我们将中央银行和审慎监管当局统称为“货币监管相关当局”。

反洗钱监管并非传统意义上的金融监管，最初是20世纪70年代美国为应对日益严重的毒品犯罪而对银行设定反洗钱义务，其目的在于预防和发现利用金融体系的犯罪活动。〔48〕

我们根据美国对虚拟货币的多重监管的事实，〔49〕参照前述朱玮、吴云和杨波的结论，认为虚拟货币具有三种属性：从货币的角度，虚拟货币可以执行货币作为价值储藏手段、交易媒介和计价单位的职能；从投资的角度，虚拟货币是证券投资（或者至少是一种需要被监管的投资）；

〔46〕 See Sean Foley，Jonathan R. Karlsen，Talis J. Putnins，Sex，Drugs，and Bitcoin：How Much Illegal Activity Is Financed Through Cryptocurrencies? 32（5）*Rev. Financial Stud.*，1798，1798－1853（2019）.

〔47〕 也有研究认为比特币从事非法活动数量可能不多。美国麻省理工学院IBM沃森人工智能实验室利用人工智能对20万个比特币节点的23万个支付流和166种特征进行了深度学习，只发现其中2%从事非法活动、21%从事合法活动。但由于对其余77%无法进行有效识别，该研究说服力不强。（See Mark Weber et al.，Anti-Money Laundering in Bitcoin：Experimenting with Graph Convolutional Networks for Financial Forensics，arXiv：1908. 02591，Submitted on July 31，2019，available at https://arxiv.org/abs/1908. 02591，last visited on Jun. 10，2020.）

〔48〕 在不同国家，可能由不同的部门对金融机构实施反洗钱监管，包括：中央银行（如中国）、财政部（如美国）、警察部门（如澳大利亚）、金融行为监管部门（如英国）、单设专门部门（如俄罗斯）等。

〔49〕 参见前引〔16〕，孙国峰、陈实文。

从反洗钱角度，虚拟货币是价值转移的手段。〔50〕

虚拟货币执行货币职能与价值转移手段职能二者紧密联系，虚拟货币正是因为可以充当交易媒介，所以可以替代法定货币进行价值转移。按照实质优于形式的原则，2013 年美国财政部就将虚拟货币纳入了反洗钱监管。〔51〕这个原则被 FATF 制定的国际反洗钱标准所吸收。

虚拟货币可以执行货币职能、可以作为价值转移的手段较为容易理解，但是，在直觉上虚拟货币与通常的证券（股票、债券）相差极大。美国 SEC 在阐述监管政策时指出，传统的证券确实是基于企业或公司利益的，但这并不是证券的本质所在，SEC 仍然坚持用“豪威标准”（Howey test）四要件判断是否属于证券。〔52〕由于虚拟货币性质讨论并非本文重点，本文在此仅作一般说明，国内有大量关于 ICO 研究的论文可以参考。〔53〕

虚拟货币所面临的金融监管问题的汇总可参见表 2。

表 2　　虚拟货币面临的金融监管问题

性质	监管内容	监管当局	具体监管者举例	虚拟货币有关的监管问题
货币〔54〕	支付和清算，法定清偿手段	中央银行	中国人民银行，英格兰银行	尚未对法定货币体系形成冲击
	金融稳健性	审慎监管当局	中国人民银行（宏观）、中国银保监会（微观）；英格兰银行	对金融审慎的问题尚处在概念讨论阶段
证券〔55〕	投资者保护、市场秩序	金融行为监管当局	中国证监会；英国金融行为监管局（FCA）；美国证券交易委员会（SEC）	是否适合普通投资者存在巨大争议；主要面临的问题是欺诈、价格操纵
价值转移手段	反洗钱	反洗钱监管当局	中国人民银行；美国财政部；英国金融行为监管局（FCA）	被洗钱和犯罪活动利用已经相当严重，具有监管的迫切性

（二）反洗钱先行的内在逻辑

对虚拟货币货币属性、证券属性和价值转移手段属性的三种监管在现阶段面临的急迫性和必

〔50〕 参见前引〔4〕，朱玮、吴云、杨波书，第 271－283 页。

〔51〕 See Financial Crimes Enforcement Network，Application of FinCEN's Regulations to Persons Administering，Exchanging，or Using Virtual Currencies，United States Department of the Treasury（March 2013）. 美国财政部认为，提供虚拟货币价值转移服务在性质上和已有的货币服务业务（money service businesses，MSBs）没有本质区别，因此要适用相同的反洗钱监管标准。

〔52〕 See SEC Chairman Jay Clayton，Statement on Cryptocurrencies and Initial Coin Offerings（Dec. 11，2017）. 豪威规则四要件的具体运用可参见 SEC，Framework for“Investment Contract”Analysis of Digital Assets（April 3，2019）。

〔53〕 如前引〔12〕，孙国峰、陈实文；张美慧：《境外市场证券法视野下的代币发行监管——基于美国、新加坡、澳大利亚和中国香港地区的监管实践》，载《财经法学》2019 年第 3 期，该文深入运用多个国家和地区的监管规则分析了虚拟货币的证券属性。

〔54〕 美国银行业的监管体系较为复杂，涉及审慎监管职能的包括美联储、财政部下设货币监理署（OCC）、联邦存款保险公司（FDIC），为简化问题，表中略去有关内容。

〔55〕 证券行业通常被认为是“资本中介”，自身并不经营风险，风险由投资人承担，证券行业仅在自己作为交易对手方等少数情况下存在审慎监管的问题。金融监管对审慎问题关注的焦点是银行和保险，实践中证券业的行为监管和审慎监管一般由同一个监管者负责。（参见吴云、张涛：《危机后的金融监管改革：二元结构的“双峰监管”模式》，载《华东政法大学学报》2016 年第 3 期。）

要性是不同的。

1. 虚拟货币并未对法定货币体系形成冲击：货币相关当局的容忍

在作为价值储藏手段和交易媒介时存在的天然缺陷，导致虚拟货币并未对现有货币体系形成值得关注的冲击或影响。各国在坚持法定货币作为唯一法定清偿手段的前提下，基本采取了容忍态度（除少数绝对禁止的国家）。

同时，数字货币（包括私人发行的虚拟货币和中央银行发行的“央行数字货币”）出现后，传统的金融中介（如银行）是否还有存在价值、社会信用如何放大等完全处在概念讨论阶段，〔56〕因此，审慎监管也并非本阶段的问题。

总之，目前货币主权和相关的金融稳定问题并不突出，也没有监管的必要性和急迫性。

2. 虚拟货币并不适合普通投资者：公开发行的暂缓

证券监管的核心目标是保护公众投资者，只有适合公众投资风险承受能力的产品才可以公开募集和发行，才需要进行监管（否则可以豁免）。虚拟货币究竟在多大程度上适合普通投资者是始终使各国监管者困惑的根本问题，因为专业投资者对虚拟货币的内在价值也存在巨大的分歧和争议。美国尚未登记或批准任何一种面向大众的虚拟货币或虚拟货币金融产品。〔57〕2018 年 SEC 在驳回 Winklevoss 申请比特币金融产品的官方意见中指出：按照美国证券法，是否具有内在价值由投资者自己判断，但是，SEC 有权审查基础资产（比特币）市场是否可以内在地抵御欺诈和操纵（inherently resistant to fraud and manipulation）或者有充分的预防性手段抑制欺诈和操纵。比特币（基础资产）市场并不能“内在地抵御欺诈和操纵”，也没有充分的预防性手段抑制欺诈和操纵，因此，比特币为基础资产的金融产品不适合普通投资者参与。〔58〕

虚拟货币由于没有任何支持资产，〔59〕“是否具有内在价值”“如何判断内在价值”在专业投

〔56〕 See BIS, Central Bank Digital Currencies 6, CPMI Papers No. 174, March 2018, available at https://www.bis.org/cpmi/publ/d174.pdf, last visited on Jun. 10, 2020. 中文作品中对此比较通俗的介绍，可参见〔德〕约翰内斯·比尔曼：《中央银行视角下的现金与数字货币》，载《金融市场研究》2019 年第 12 期。

〔57〕 2017 年美国芝加哥商品交易所挂牌了比特币期货，但是，期货参与者是合格投资者或专业投资者。

〔58〕 See Securities Exchange Act Release No. 83723 (July 26, 2018), 83 FR 37579 (Aug. 1, 2018). 在证券发行审批制的国家，监管当局要替代投资者进行实质性判断。但是，即使美国这样的证券注册制国家，监管当局也并非完全放弃对证券的实质性审查。SEC 多次驳回以比特币为基础资产公开发行金融产品的申请。

〔59〕 这里讨论的虚拟货币内在价值问题仅限于比特币这样没有支持资产的非稳定币。以法定货币或实物资产为储备的“稳定币”（stablecoin），也叫“资产支持型稳定币”（asset-linked stablecoin）。USDT 以美元为储备资产，是最典型也是最广泛使用的稳定币。此外，脸书（Facebook）对外公布的“天秤币”（Libra）曾打算以“一篮子”货币作为储备资产；还有以商品为支持资产的虚拟货币，如 DGX（DIGIX GOLD TOKENS）以黄金作为储备资产。但是，这种稳定币需要对支持资产进行托管，一些研究对这种稳定币发行者是否有足额资产提出怀疑，如前文所引 Griffin 等（2019）。“资产支持型稳定币”稳定币值的效果取决于支持资产的币值稳定性。在广义上，“算法基础型稳定币”（algorithm-based stablecoins）也被归为稳定币，通过算法调节代币总量来保持币值稳定。当币值价格下跌时，销毁部分代币，从而维持价格稳定；反之则增加代币数量。但是，这种稳定币在实践中并未取得稳定币值的效果，典型的例子是 NuBits。当然，对“算法基础型稳定币”的定义和范围还存在一定争议，此处不赘述。［See FSB, Regulation, Supervision and Oversight of “Global Stablecoin” Arrangements: Final Report and High-Level Recommendations, 9－10 (2020); Dirk Bullmann, Jonas Klemm, Andrea Pinna, In Search for Stability in Crypto-assets: are Stablecoins the Solution? ECB Occasional Paper No. 230, 23 (2019).］

资者当中尚有巨大的分歧。著名投资家沃伦·巴菲特认为比特币是“赌博的工具”“老鼠药”。〔60〕巴菲特的理解不一定正确，但至少说明全球顶级的专业投资者群体中对比特币的内在价值也存在巨大的争议。国际社会没有就如何向普通投资者发行虚拟货币形成大范围的共识，注册或审批的正面案例不多。

3. 反洗钱监管先行

时任 FATF 主席在 2018 年公开撰文呼吁各国重视虚拟货币被犯罪活动所利用的严重性，因为“虚拟货币已经与金融犯罪手牵手”〔61〕。虚拟货币由于匿名性，欺诈和价格操纵很难被发现。反洗钱监管能够为遏制虚拟货币市场的严重欺诈和操纵创造良好的前提，从而减少普通投资者的进入障碍。反洗钱监管将在很大程度上建立一个交易的可追踪体系，可以从根本上提高识别和遏制通过虚拟货币进行的违法犯罪活动的能力，从而净化市场和交易。因此，打击虚拟货币价格操纵、欺诈和打击通过虚拟货币洗钱的两个诉求汇聚到了反洗钱监管。

（三）国际社会以反洗钱为起点的监管尝试

金融行动特别工作组（Financial Action Task Force，简称“FATF”）是国际反洗钱标准的制定者，〔62〕从 2013 年起，FATF 着手对虚拟货币的洗钱风险进行研究。2014 年 6 月 FATF 发布了《虚拟货币：关键定义和潜在反洗钱、反恐怖融资风险》（Virtual Currencies：Key Definitions and Potential AML/CTF Risks）的报告，梳理了相关定义并结合刑事案例对虚拟货币洗钱进行了研究。2015 年 6 月 FATF 发布了《以风险为基础的虚拟货币指引》（Guidance for a Risk-based Approach to Virtual Currencies），对 FATF 标准如何适用于虚拟货币进行了探讨。

经过长期研究和讨论，在 FATF 框架下各国当局就虚拟货币反洗钱监管达成了共识。2019 年 6 月 FATF 全体会议通过了虚拟货币监管标准和配套监管指引《以风险为基础的虚拟资产和虚拟资产服务提供商指引》（Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers，以下简称《FATF2019 虚拟货币指引》），并且着手对各国执行情况进行评估。这是所有国际组织中，制定并通过的第一个针对虚拟货币的监管标准，形成了虚拟货币反洗钱监管的国际共识。

---

〔60〕 See Yun Li，Warren Buffett Says Bitcoin is a “Gambling Device” with “a lot of Frauds Connected with It”，CNBC，May 4 2019，at Market，available at https：//www. cnbc. com/2019/05/04/warren-buffett-says-bitcoin-is-a-gambling-device-with-a-lot-of-frauds-connected-with-it. html，last visited on Jun. 10，2020.

〔61〕 Marshall Billingslea，Virtual Assets and Financial Crime Now Go Hand in Hand，Financial Times，Oct. 28，2018，at Opinion.

〔62〕 FATF 成立于 1989 年，最初是“七国集团”峰会为应对洗钱危害、预防并协调反洗钱国际行动而发起设立的政府间国际组织。经过长期演变，其已经成为国际反洗钱标准的制定机构。目前，FATF 有 39 个正式成员（含两个国际组织），全球共超过 200 个国家和地区加入了 FATF 或 FATF 框架下的区域反洗钱组织。FATF 秘书处设在经济合作与发展组织（OECD）巴黎总部。参见 FATF 官方网站的介绍，载 https://www.fatf-gafi.org/about/，最后访问时间：2020 年 6 月 10 日。中国是 FATF 成员，同时是 FATF 框架下区域性反洗钱组织“欧亚反洗钱组织”（EAG）和“亚太反洗钱组织”（APG）的成员。FATF 已经组织完成三轮世界范围内的反洗钱评估，目前正在进行第四轮反洗钱评估。中国分别于 2007 年和 2019 年通过 FATF 第三轮和第四轮反洗钱评估。

四、虚拟货币反洗钱国际监管标准及其影响

（一）反洗钱监管的国际标准概述：带有“牙齿”的强制性规则

FATF 标准由“四十项建议”组成，每项建议及其释义具有同等效力。〔63〕为了评估各国执行“四十项建议”的情况，FATF 发展了一套完整严密的“评估方法”，包含四十个合规性指标（对应“四十项建议”），十一个有效性指标（从“四十项建议”中整合而出），每个指标下一般有十几个分项指标。〔64〕

FATF“四十项建议”的特点是围绕反洗钱设定一系列的要求，包括刑事司法、反洗钱监管、国际合作、执行联合国定向金融制裁四个方面，涵盖了从司法、执法、监管到外交的各个领域。

FATF“四十项建议”对全球 200 多个经济体均有约束力。与以往国际组织不同，FATF 通过成员之间相互评估的方式督促成员履行标准，对于不能达标的成员，将采取金融抵制和反制措施，实同金融制裁。由于 FATF 的核心发起国家掌握了全球主要的可自由兑换货币和跨国支付结算系统，这些国家联合起来实施金融制裁，足以将任何经济体隔绝在世界金融体系之外，威力远超过传统的经济制裁或贸易制裁。这一整套带有“牙齿”的评估机制，使得 FATF 的反洗钱标准成为具有实质性强制约束力的国际标准。

2019 年 6 月，FATF 通过在“建议 15（新技术）”中新增“释义”的方式，具体规定了虚拟货币监管的要求。标准采用一种“连锁”（cascading）影响的方式，具体列举现有哪些“建议”适用于虚拟货币以及如何适用虚拟货币。2019 年 10 月，FATF 根据修订后的“四十项建议”修改了“评估方法”。根据 FATF 全会的决定，FATF 首先在 2020 年 6 月完成对各国（地区）执行情况的初步审查，在此基础上再组织针对性全面评估。

FATF 新通过的虚拟货币反洗钱监管标准，涉及行业准入、反洗钱监管要求、国际合作等，对虚拟货币的运行模式和行业发展具有直接的革命性影响。

（二）虚拟货币反洗钱监管的具体要求

1. 尊重各国对于虚拟货币合法性的态度

为防止外界对虚拟货币合法性的误解，FATF 将“虚拟货币”改称“虚拟资产”，并发表了声明澄清不对虚拟货币合法性进行背书。〔65〕

类似于 FATF 对赌场的监管要求，如果一国能够有效禁止虚拟货币，则不需要进行监管，反

〔63〕“四十项建议”的全称是《打击洗钱、恐怖融资和扩散融资的国际标准》［International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation（amended June 2019）］，业内一般将其称为“FATF Recommendations 2012”“四十项建议”。

〔64〕“评估方法”的全称是《评估 FATF 建议技术性合规和反洗钱、反恐怖融资体系有效性的方法》［Methodology for assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems（amended October 2019）］，业内一般将其称为“Methodology 2013”“评估方法”。

〔65〕 See FATF Statement，Regulation of Virtual Assets（Paris，France，Oct. 19，2018）.

之，则需要设立监管规则并有效监管。〔66〕

2. 适用对金融活动和金融机构的监管标准对虚拟货币活动及其服务提供商进行监管

现有的反洗钱监管规则的基本框架是，通过给义务机构（包括金融机构和“特定非金融机构”〔67〕）设定反洗钱预防义务构建反洗钱体系，反洗钱监管当局的主要目标是督促义务机构履行反洗钱义务。FATF 在原有的两类义务机构的基础上，创设了第三类义务机构：虚拟资产服务提供商（Virtual Assets Service Provider，VASP）。从技术中立的立场出发，FATF 的监管基本原则是，适用金融机构和金融活动的标准都适用于虚拟资产服务提供商和虚拟资产活动。〔68〕

虚拟资产服务提供商承担与银行一样的反洗钱义务（“建议 10”至“建议 21”共 12 条标准），其核心的三项义务包括：客户尽职调查，〔69〕保存客户资料和交易资料，向国家指定的金融情报中心提交可疑交易报告。虚拟资产服务提供商与银行关于活动性质、活动内容、反洗钱义务的对比请参见表 3。

表 3　　虚拟资产服务提供商与银行对比

	银行（典型反洗钱义务主体）	虚拟资产服务提供商（VASP）
活动性质	价值转移	
活动内容	法定货币保管、控制	虚拟货币的保管和控制
反洗钱义务	反洗钱三项核心义务等	

3. 监管的范围包括所有虚拟资产活动

FATF 监管规则通过活动的实质来定义机构，虚拟资产服务提供商是为虚拟资产活动提供服务且作为营业（as a business conduct）的机构或个人。为便于理解，《FATF2019 虚拟货币指引》中列举了主要的“虚拟资产活动”，包括：（1）法定货币和虚拟货币之间兑换；（2）不同种类虚拟货币之间兑换；（3）虚拟货币转移；（4）保存、管理虚拟货币；（5）参与虚拟货币发行和销售，或者为其提供服务。在此之前，一些国家仅对虚拟货币和法定货币直接兑换过程进行反洗钱监管，FATF 标准将所有虚拟货币转移活动纳入了监管范围，尤其是虚拟货币之间的转移活动。

〔66〕 See FATF，Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers，paras. 32，67 (June 2019).

〔67〕 FATF 框架下的非金融机构被称为“特定的非金融行业和职业”（Designated Non-Financial Businesses or Professions），缩写为“DNFBPs”，中文官方标准译法为“特定非金融机构”，通常包括律师、会计师、房地产经纪等。

〔68〕 讨论过程中，秘书处提出的方案是：直接将虚拟资产活动纳入金融活动范畴，将虚拟资产服务提供商纳入“金融机构”的范畴，这样，原有的规则将自动适用。与会代表同意这个监管思路，但是，有代表提出这种安排在技术上过于笼统，不能解决虚拟货币的特殊问题和关切。因此，最后达成的方案是在“建议 15”中增加“释义”，具体列明现有的哪些规则适用，哪些规则按照更高的要求适用。

〔69〕 根据“建议 10”的规定，客户尽职调查（customer due diligence）比我们通常所说的“客户实名制”要求更加广泛，不仅包括核实客户身份准确性，还包括穿透识别法人客户背后的最终控制自然人或最终拥有自然人，了解客户业务的目的和性质等。

理解虚拟资产活动的关键是理解“托管钱包”，“托管钱包”是 FATF 设置规则的“假象典型”。FATF 在列举上述虚拟资产活动范围时，已经推定了上述活动中，服务提供商通过“托管钱包”获得了虚拟货币的控制权。“托管钱包”类似于银行账户，用户将虚拟货币的私钥储存在“托管钱包”中，服务商获得了私钥的控制权，用户通过指令可以要求服务商对“托管钱包”中的虚拟货币进行转移。

如果用户不通过第三方保管和使用虚拟货币，那么他使用的是“非托管钱包”，“非托管钱包”可以理解为存放现金的保险柜，是由个人自己控制的存储手段。提供“非托管钱包”服务类似于提供现金保险柜，提供的是技术服务，不属于反洗钱监管范围。

现有货币体系和虚拟货币体系下，是否通过第三方保管和使用法定货币或虚拟货币，带来的反洗钱义务范围对比，请参见表 4。

表 4　　典型反洗钱义务范围对比

	现有货币体系	虚拟货币体系	说明
自我保管和使用	使用者自己持有现金（保险箱）	使用者自己持有私钥（非托管钱包）	提供现金保存手段的机构（如保险箱制造商）不是反洗钱义务机构；类似地，仅提供个人保管和使用虚拟货币有关技术服务的机构也不是反洗钱义务机构
通过第三方保管和使用	使用者通过银行（银行账户）	使用者通过虚拟货币服务商（托管钱包）	银行是价值转移执行者，是反洗钱义务机构；类似地，虚拟货币服务商属于反洗钱义务机构

虚拟货币托管钱包与银行账户、证券账户的对比请参见表 5，将有利于理解“托管钱包”。

表 5　　虚拟货币托管钱包与银行账户、证券账户的对比

	银行账户	证券账户	虚拟货币托管钱包
保管对象	法定货币	证券	虚拟货币
保管控制方式	银行对账户中资金进行保管、控制	证券经纪商对账户中证券进行保管、控制	钱包提供商对托管钱包中资产进行保管、控制
交易方式	根据用户指令	根据用户指令	根据用户指令
政府公权力行使	监管机关可以通过银行账户对资金流向实施监控，政府可以依法指令银行冻结账户资产	监管机关可以通过证券账户对证券资产流向实施监控，政府可以依法指令证券经纪商冻结账户资产	监管机关可以通过托管钱包对资金流向实施监控，政府可以依法指令虚拟货币服务商冻结账户资产

我们常说的“虚拟货币交易平台”就是典型的虚拟资产服务提供商。〔70〕

4. 设置行业准入门槛，防止游离监管之外

FATF 对行业准入设置了门槛要求，一国要根据情况采取注册制或审批制，虚拟资产服务提

〔70〕 另外，还出现了物理形态的电子终端（physical electronic terminals），如比特币自动取款机（bitcoin ATMs）等，对于通过这些物理终端机器购买、转移虚拟货币的活动，也适用 FATF 关于虚拟货币监管的规则。平台如果仅发布价格信息，不从事任何交易活动，则不属于受监管活动。关于监管范围，可参见前引〔66〕，FATF 文，第 33－54 段。

供商必须获得注册或许可后方可提供服务。具体而言，成立地、运营地、客户所在地都可以要求服务商向其申请注册或许可。服务商是非自然人时，其成立地必须要求其申请注册或许可；服务商是自然人时，其营业地须要求其申请注册或许可。对于服务商注册地提出强制性要求的动议，由中国等发起，针对的是防止离岸服务（在一个辖区注册，但为另一个辖区提供服务）游离于监管之外，防止形成“监管天堂”或“监管洼地”。〔71〕

5. 强化国际合作，防止监管套利

“建议 37”至“建议 40”分别规定了司法协助、跨境资产冻结和没收、引渡、其他形式的国际合作。其中，“建议 37”“建议 38”“建议 39”规定的是刑事司法协助，“建议 40”是正式的刑事司法协助以外的其他合作，主要是双边反洗钱监管合作和双边反洗钱金融情报交换。FATF 为了全面加强在虚拟货币领域的国际合作，将相关要求扩大化到所有监管领域（不限于反洗钱领域）。其规则指出，对虚拟货币监管机关不同，对虚拟货币性质、称谓不同，都不应影响各国进行监管信息交换，〔72〕从而防止监管套利。

6. 监管标准更为严格的适用

FATF 认可虚拟资产更高的内在风险，因此，按照风险为本的要求对某些标准适用更为严格，主要在两个方面：

一是 FATF 标准要求对于金融机构必须由政府机构实施监管，对于非金融机构可以由自律组织进行监管。鉴于虚拟资产服务的特殊风险状况，FATF 要求只能由政府机构对其实施监管。

二是鉴于虚拟货币具有跨国性特点和较高的洗钱内在风险，将虚拟资产的价值转移统一推定为跨国交易，并实施比现有跨国交易更加严格的反洗钱要求。根据 FATF 标准，对于偶发性（occasional）交易，当交易额（无论国内或跨国）达到 1.5 万美元或欧元（孰低）时金融机构必须实施客户尽职调查，当跨国交易达到 1000 美元或欧元（孰低）时金融机构必须核实客户身份的准确性（客户尽职调查的一个方面）。新的标准进一步要求，涉及虚拟货币的偶发性交易，只要达到 1000 美元或欧元（孰低）就必须实施客户尽职调查。

（三）反洗钱国际标准对行业生态的革命性影响

只有个人之间通过“非托管钱包”（完全是个人之间的点对点交易，不借助任何外部服务）的交易在监管之外，任何交易通过第三方服务进行，都将纳入监管体系之内。这符合基本的监管逻辑和行业技术特点。“非托管钱包”对使用者有很高的技术要求，如果缺乏相应技术，不仅很难正确交易，而且容易丢失虚拟货币，因此，其仅限于少数人使用。监管主要关注的是营业性活动，而不是个人之间的行为。个人不借助任何外部服务的点对点交易很难被发现，类似于大众的现金交易，对于这些行为的监管不符合监管的成本收益原则。

---

〔71〕 中国在建议中提出，成立地有首要的（primary）监管义务。秘书处在吸收各个成员意见基础上，将表述改为“at a minimum”（作为最低要求）。

〔72〕 FATF“建议 15 释义”第 8 段第 2 句话规定：“尤其是，虚拟资产服务商的监管机关应当立即和建设性地与外国对应机关交换信息，不应受制于双方监管机关的性质、地位以及对服务商的不同称谓和地位。”

FATF 规则设置了基本的准入门槛，防止了行业“裸奔”状态。而且，为了防止跨辖区的监管套利，FATF 要求成立地必须实施行业准入，而且强化了国际合作要求。

根据 FATF 规则，服务商要对所有客户进行实名制登记，对交易背景和目的进行审查，将可疑交易信息报告给政府，反洗钱监控全面植入虚拟货币交易服务，国家“追踪资金”的范围延伸到虚拟世界。

监管对于虚拟货币在投资者适当性方面的担忧，很大一部分来源于虚拟货币缺乏可追踪性。随着反洗钱基础设施的建立，各国证券当局可能会允许虚拟货币在一定条件下成为公众可投资的金融产品。

五、监管的展望：从“外部活动”到“内部治理”

（一）“外部活动”与“内部治理”：反洗钱规则的局限性

我们可以将一个虚拟货币自我运转的社群类比于一个上市公司，“链上治理”指的是这个社群的内部的治理，包括代码修改的规则、增加虚拟货币总量规则、“分叉”（部分矿机用脚投票，在原有链的基础上形成新的链）等，这些内部的投票活动很大程度上和公司内部治理具有相似性。“链上交易”活动相当于上市公司的股票在公司之外的发行和流通。上市公司与虚拟货币社群有关活动的对比，请参见表 6。

表 6　　上市公司和虚拟货币社群有关活动的对比

	上市公司	虚拟货币社群	现有监管规则
内部治理（链上治理）	章程修改	代码规则修改	实践空白
	股票增发	增加虚拟货币总量	实践空白
	公司分立	“分叉”	实践空白
外部活动（链上交易）	股票发行	ICO	仅有反面实践
	交易规则（防止价格操纵等）	交易规则（防止价格操纵等）	仅有反面实践
	作为价值转移手段	作为价值转移手段	完整监管规则

我们现有的反洗钱监管规则仅限于作为价值转移手段时的外部活动。主要国家监管当局并未正面审批或注册通过任何一种虚拟货币作为公开发行的金融产品，因此，对虚拟货币内部治理的实践完全空白。目前已有的实践，仅有对操纵市场和未经审批或注册发行虚拟货币两种行为的打击。

比特币创造了“代码即法律”的社群治理模式。菲利皮（Filippi）和洛夫拉克（Loveluck）以比特币治理为例将区块链治理分为两个层次，“以基础设施进行治理”和“对基础设施进行治

理”，两者是相互作用的，最终的体现在于“对基础设施进行治理”，也即对代码的修改。〔73〕对代码规则的修改类似于上市公司章程的修改，是治理中最高的权力/权利，是其他权力/权利的基础。

对于内部治理，只有当虚拟货币通过监管当局审批或注册时，才可能将现有的证券监管规则运用到区块链治理中去。非中心化的治理秩序在多大程度上能够实现良好的治理，需要在现有法律框架下继续尝试。

（二）“内部治理”：未来的根本性挑战

对于监管者而言，链上的内部治理将是全新的议题，至少面临以下三个根本性挑战：

首先，从应然性的角度，“什么是良好的治理”？公司治理的标准在多大程度上适用于自治社群？监管在多大程度上允许不同治理模式的探索？区块链自治社群的时间远短于公司存在的时间，已有的经验和案例相当少，这注定是一个反复探索的过程。

其次，从责任承担的角度，自治社群本身不存在有形实体和组织架构，监管者如何找到监管对象和义务主体？公有链的参与者是可以匿名的（上述反洗钱规则并不要求区块链参与者实名制，只是参与者通过第三方对外发生交易时才需要在服务商进行实名制登记），而且自治社群并不存在有形的组织架构，究竟谁来履行监管规定的义务？如何识别义务履行者？“道”（Dao）平台尝试了“非中心化自治组织”的理想，尽管其发行“道币”行为被美国 SEC 认定为未经注册发行证券行为而叫停，但是引发了如何界定区块链自治社群中新型组织的法律性质和责任承担这两个根本性问题。〔74〕

最后，从法律执行的角度，区块链社群是依据代码的治理，监管者如何强制自治社群修改代码？法律应当赋予监管者“超级代码控制者”的权力吗？“超级代码控制者”修改代码后，社群参与者会选择用脚投票吗？

（三）展望：相信试错的力量

从系统自发维持的角度，比特币的社群自治实验无疑是成功的，在一个没有暴力维持运营、没有第三方权威的社群中，比特币、以太币社群自发形成全球性的、千亿美元规模的金融体系。但是，从普通参与者的角度，尽管比特币的理想是建立一种非中心化秩序，然而比特币，及其后来的以太币、“非中心化自治组织”尝试的“道”在治理结构上都是一种中心化结构，虚拟货币社群还存在严重的决策权力集中、普通用户难以发声的治理缺陷。

中心化和非中心化治理的平衡点，表面上看是公司治理、社群治理的问题，但背后是人类政

---

〔73〕 See Primavera De Filippi，Benjamin Loveluck，The Invisible Politics of Bitcoin：Governance Crisis of a Decentralized Infrastructure，5（4）*Internet Pol'y Rev.*，（2016），available at https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure，last visited on Jun. 10，2020.

〔74〕 如果从既有法律中推导，这种组织的法律性质应当是普通合伙。法人、有限合伙的设立在绝大部分国家以登记为前提，“道”没有登记，因此不能构成法律上的法人、有限合伙；普通合伙不以登记为前提，可以基于共同的合同行为而产生，所有参与者要承担无限连带责任。至少在美国法框架下，认定该组织为合伙，并不影响其 ICO 行为构成证券发行。［See Laila Metjahic，Deconstructing the DAO：The Need for Legal Recognition and the Application of Securities Laws to Decentralized Organizations，39 *Cardozo L. Rev*，1533，1533－1568（2017）.］国内学者普遍认为，普通参与者不应当承担无限连带责任，因此比较适合将其认定为“有限合伙”。（参见汪青松：《区块链系统内部关系的性质界定与归责路径》，载《法学》2019 年第 5 期。）

治哲学的永恒难点，自古希腊以来西方政治哲学对此问题一直没有固定不变的最优解。从动态的角度看，也许十年时间还太短，我们不能以一时的治理困局就否定竞争和进化的力量，毕竟虚拟货币的用户掌握了用脚投票的权利，私人竞争的长期存在，给反复试错提供了可能性。

对虚拟货币的反洗钱监管，可以提高虚拟市场预防和抵御欺诈、操纵的能力，为虚拟货币公开发行提供良好的市场前提。如果虚拟货币发行可以得到国家的认可，那么国家监管的规则也将会随之强行植入虚拟货币社群，现有的证券投资者保护规则在多大程度上适用于区块链社群以及监管的边界、容忍度、手段都将是全新的挑战。我们相信，国家监管所代表的现实世界的法律和虚拟世界的技术规则在动态的博弈中可能会最终产生意想不到的成功治理模式。

Abstract：Ten years after the birth of virtual currencies（VCs），they still have not introduced significant impact over the fiat currency systems，then the major monetary authorities do not prohibit individuals from holding or using VCs. At the same time，the major securities authorities also do not register or license to the public any virtual currencies or financial products based on VCs，because the investment suitability of VCs is still unclear. However，the authorities must address the serious speculations，frauds and money laundering in a substantial way. Under the promoting and leading of the Financial Action Task Force（FATF），the global society finally reached consensus on anti-money laundering（AML）regulation over VCs in 2019. The new regulatory framework will fundamentally change the autonomy of VCs communities in the world. While the AML rules only cover the regulation over the activities out of blockchain to prevent ML，and the governance of blockchain will be the core issue and biggest challenge for further regulation in the next stage.

Key Words：virtual currencies，anti-money laundering regulation，governance of blockchain

（责任编辑：缪因知　赵建蕊）

财经法学 No. 6，2022
pp. 111 - 124

自由贸易协定金融信息传送规则构建

马　光　卜小翠*

内容提要：在国际贸易法框架下，金融信息传送规则中最核心的“金融信息传送”条款源起于乌拉圭回合一揽子协定中《关于金融服务承诺的谅解》中的“信息传送和信息处理”条款，后在各FTA中也相继出现。数字经济背景下，对跨境数据流动规制的关注开始集中于电子商务和数字贸易领域，“金融信息传送”条款也因此在近年来的FTA中被电子商务或数字贸易的跨境信息传送规则所吸收。然而一体化规制方法仍然存在许多基础性问题待解决，应当谨慎看待。现阶段，“金融信息传送”条款已经发展出了“金融信息传送自由原则＋个人数据、个人隐私、个人记录和账户机密性例外＋有限度的监管例外”的基本结构，并在数据本地化问题下衍生出了“金融服务计算设施所在地规则”。中国应在坚持数据主权立场的基础上，升级FTA金融信息传送规则，从国际规则遵守者向国际规则制定者转变，以期维护本国在金融服务领域和数字科技领域的进攻利益。

关键词：跨境数据流动　金融信息传送　FTA金融信息传送条款　金融数据出境

一、引言

全球数字化背景下，跨境数据流动成为推动全球经济发展的重要力量。麦肯锡全球研究院2016年的报告指出：“实物商品和资金的流动曾是20世纪全球经济的标志，但如今这些流动已经趋于平缓或下降。21世纪的全球化越来越被数据和信息流所定义。数据和信息流几乎支撑了传统

* 马光，浙江大学光华法学院副教授、浙江大学国际法研究所执行所长；卜小翠，浙江大学光华法学院硕士研究生。

本文为国家社会科学基金重大项目“建立健全我国网络综合治理体系研究”（20ZDA062）、浙江省科技计划项目“智能司法开放创新平台开发及应用示范——基于人工智能的司法服务平台及示范应用”（2020C01060）的阶段性成果，浙江省法学会2022年度法学研究课题“涉外企业合规风险控制研究”（2022NB14）的成果。

贸易中的所有跨境交易，同时在世界各地传递着思想和创新。”〔1〕跨境数据流的惊人增长和潜在经济效益已经引起了全球监管者对跨境数据流动规制的广泛关注。从实践来看，国际社会目前的共识是：贸易协定是管理跨境数据流的适当场所。因为当信息跨境流动时，这些流动似乎基本上与贸易相关。〔2〕

国际贸易法对跨境数据流动的关注最早出现在电信、金融等特定服务部门。其中，以乌拉圭回合一揽子协定中《关于金融服务承诺的谅解》（以下简称为《谅解》）〔3〕的“信息传送和信息处理”条款最为典型。根据《谅解》，以经济合作与发展组织（以下简称 OECD）成员国为主的 34 个世界贸易组织（以下简称为 WTO）成员自愿作出更高水平的金融服务开放承诺，且此类承诺按照最惠国待遇适用于所有 WTO 成员。〔4〕随着电子商务和数字贸易的日渐兴起，一方面，由于 WTO 在制定规则以应对世界经济中与数据相关的变化上停滞不前，世界主要经济体逐渐转向以自由贸易协定（以下简称为 FTA）作为规则升级的主要平台，《谅解》金融信息传送条款也随之被众多高标准 FTA 所吸收；另一方面，自《美国—韩国 FTA》首次在电子商务章节纳入跨境信息流动条款后，对跨境数据流动规制的关注开始集中于电子商务和数字贸易领域，并在近年来的 FTA 中呈现了跨境信息传送一体化规制的趋势。〔5〕由此提出的问题是：金融信息传送是否还有单独规制的必要。

当前，除《区域全面经济伙伴关系协定》（以下简称为 RCEP）外，中国已签署的 16 个 FTA 皆未规定金融信息传送条款。〔6〕关于我国已签订 FTA 金融信息传送规则设置情况请参见表 1。就文本而言，这些 FTA 仍有较大完善空间。鉴于我国已基于 RCEP 条款承诺金融信息传送，跨境金融数据流动议题也已在不同程度上为各处于磋商阶段的区域及双边经贸协定所触及，深化对该条款的探究，提出关于中国在该议题上的主张的建议具有突出现实意义。

有鉴于此，本文将分析梳理 FTA 金融信息传送规则的发展脉络，进而结合各国治理动向，揭示各国数据治理日渐趋同的现象，并深入探析金融信息传送规则的逻辑构建。在此基础上，本文将根据中国的基本立场，详细擘画中国应采取何种条款表达。

---

〔1〕 See Mckinsey Global Institute, Digital globalization: The new era of global flows, Report (Feb. 24, 2016), available at https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization- the-new-era-of-global-flows, last visited on May 2, 2022.

〔2〕 See Susan Ariel Aaronson, Data Is Different, So Policymakers Should Pay Close Attention to Its Governance, in Mira Burri ed., *Big Data and Global Trade Law*, Cambridge University Press, 2021, p. 342.

〔3〕 值得说明的是，《谅解》与《服务贸易总协定金融服务附件》（以下简称为《GATS 金融服务附件》）为两个不同的法律文件，《GATS 金融服务附件》属于 GATS 的一部分，而《谅解》不是 GATS 的一部分，但被附加到乌拉圭回合的最后文件中。中国未签署《谅解》。

〔4〕 See Chantal Thomas, Globalization in Financial Services—What Role for GATS, 21 *Annual Review of Banking Law* 323, 324 (2001)，转引自杨幸幸：《〈美墨加协定〉金融服务规则的新发展——以 GATS 与 CPTPP 为比较视角》，载《经贸法律评论》2019 年第 4 期。

〔5〕《澳大利亚—新加坡数字经济协定》（以下简称为 ASDEA）、《美国—日本数字贸易协定》（以下简称为 USJDTA）及《WTO 电子商务谈判合并文本》（以下简称为《合并文本》）、《欧盟—澳大利亚/新西兰贸易协定》谈判中欧盟方面提交的初始文本皆采取了此种安排。

〔6〕 中国与毛里求斯、韩国、澳大利亚、新加坡、智利的 FTA 中单设电子商务章节，但电子商务章节也未设置信息传送相关条款。

表 1　　中国已签订 FTA 金融信息传送规则设置情况汇总表

<table>
<tr><th>类别</th><th>名称/参与方</th><th>金融信息传送
条款定位</th><th>其他金融信息
相关条款</th><th>中方金融
服务承诺</th></tr>
<tr><td>多边
FTA</td><td>RCEP（含中国、日本、韩国、澳大利亚、新西兰、东盟十国）</td><td>第八章　附件一“金融服务”
第九条　“信息传送与信息处理”</td><td rowspan="11">（1）定义条款：
金融服务包括以下活动：其他金融服务提供者提供和传送金融信息、金融数据处理及相关软件。
（2）特定信息处理条款或国内法规条款：
本协定的任何条款/本章的任何规定不得解释为要求一缔约方披露与个人客户相关的事务和账户信息，或公共实体拥有的任何机密或专有信息。</td><td rowspan="12">在“跨境提供”方式下：
提供和传送金融信息、金融数据处理以及与其他金融服务提供者有关的软件。</td></tr>
<tr><td rowspan="11">双边
FTA</td><td>中国、韩国</td><td>单设第九章“金融服务”章节，未规定信息传送条款</td></tr>
<tr><td>中国、毛里求斯</td><td rowspan="4">“金融服务”作为“服务贸易”章节的章节或附件，未规定信息传送条款</td></tr>
<tr><td>中国、格鲁吉亚</td></tr>
<tr><td>中国、澳大利亚</td></tr>
<tr><td>中国、瑞士</td></tr>
<tr><td>中国、冰岛</td><td rowspan="8">设“服务贸易”章节，在条文中纳入《GATS 金融服务附件》</td><td rowspan="8">定义条款：
金融服务包括以下活动：其他金融服务提供者提供和传送金融信息、金融数据处理及相关软件。</td></tr>
<tr><td>中国、东盟（含文莱、柬埔寨、印度尼西亚、老挝、马来西亚、缅甸、菲律宾、新加坡、泰国、越南）</td></tr>
<tr><td>中国、新加坡</td></tr>
<tr><td>中国、巴基斯坦</td></tr>
<tr><td>中国、柬埔寨</td></tr>
<tr><td>中国、秘鲁</td></tr>
<tr><td>中国、新西兰</td><td rowspan="3">或明确已签署协定不适用于金融服务，或无相关规定也未明确纳入 GATS 金融服务规则</td><td rowspan="3">无</td></tr>
<tr><td>中国、智利</td><td rowspan="2">未承诺金融服务开放</td></tr>
<tr><td>中国、哥斯达黎加</td></tr>
<tr><td>中国、马尔代夫</td><td colspan="3">无公开文本</td></tr>
</table>

二、FTA 金融信息传送规则发展脉络

（一）FTA 金融信息传送规则体系

金融服务的提供与金融信息密不可分。系统来看，FTA 对金融信息传送问题的规制主要包括三部分。

一是以金融服务定义条款为基础的金融信息传送承诺。涉及金融服务内容的 FTA 大多沿袭了 GTAS 对金融服务的范围界定：“金融服务包括提供和传送其他金融服务提供者提供的金融信息、金融数据处理和相关软件的活动。”也即，如有关国家在金融服务类别下进行了承诺，则须保证相应的金融信息传送可实现。如《新西兰—新加坡更紧密经济伙伴关系协定》规定：“跨境

提供模式的承诺仅限于：提供和传送上文（k）段所述的金融信息和金融数据处理……不包括中介服务。”《韩国—新加坡 FTA》承诺：“外国银行的新加坡分行可以将数据传送到其总部和姐妹分行进行处理，前提是存在适当的控制措施，数据/信息的完整性和保密性得到保障，并且允许新加坡金融管理局在处理数据/信息的地方现场访问数据/信息。”我国在中韩、中澳等多个 FTA 中承诺了“跨境提供”方式下开放“提供和传送金融信息、金融数据处理以及与其他金融服务提供者有关的软件”。美国在与新加坡、智利等国的 FTA 中也都承诺了此类信息传送。

二是专门以金融信息处理和传送为内容的条款，也即本文重点探讨的金融信息传送条款。除《谅解》以外，《新加坡—澳大利亚 FTA》最早采纳了类似的明确规定：“任何一方均不得阻止信息传送，包括通过电子方式传送数据，保护个人数据的限制除外。”《美国—新加坡 FTA》也纳入了这一规定的软化版：“根据任何一方的要求，金融服务委员会应考虑与以下事项有关的任何事项：（a）金融机构以电子或其他形式将信息转入或转出一方的领土，如该等数据处理是日常经营所需的；（b）在处理和传播个人数据方面保护个人隐私，以及保护个人记录和账户的机密性。”《印度—新加坡全面经济合作协定》《哥伦比亚—欧洲自由贸易联盟成员国 FTA》《日本—瑞士 FTA》及其后的诸多双边、多边 FTA 都在金融服务规则部分设置了该条款。

三是作为限制的“特定信息的处理”条款。该条款以传统金融信息保密要求为基础。比较典型的如《以色列—哥伦比亚 FTA》规定：“本协定中的任何内容均不得解释为要求一方披露与个人数据、个人客户事务和账户有关的信息，或公共实体拥有的任何机密或专有信息。”类似地，《哥伦比亚—巴拿马 FTA》规定：“1. 本章的任何规定均不要求一方披露或允许访问：（a）金融机构或跨境金融服务提供者的个人客户的财务和账户相关信息；或（b）披露可能会妨碍遵守法律或以其他方式违反公共利益或损害特定公司的合法商业利益的任何机密信息。2. 在不影响双方监管机构签署的谅解备忘录的情况下，为合并监管目的，双方承诺不禁止子公司及在其境内设立的子公司将信息传递给母公司所在地监管机构。前款所称信息包括反映子公司或子公司财务状况的信息，包括其资产、风险管理和公司治理情况的信息。”《加拿大—韩国 FTA》《新加坡—澳大利亚 FTA（升级版）》《欧盟—墨西哥现代化全球协定》也都包含了禁止要求披露保密信息的规则。

从特别承诺到金融信息传送条款的发展可以视作金融信息传送领域的负面清单化，反映了全球数字化经济语境下的贸易规则调适。同时，在这一背景下仍然可以看到金融发达国家与金融欠发达国家间金融开放水平的巨大差异：约有 71 个 FTA 文本包含金融信息传送相关内容，而明确设有信息处理或信息传送条款的不到半数，且缔约方主要为美国、欧盟、新加坡、澳大利亚、加拿大、日本、韩国。〔7〕此外，尽管欧盟和美国通常被视为跨境数据流动规制的两大规则制定者，但在金融信息传送领域，新加坡似乎脱颖而出，这也与新加坡高度依赖国际金融的发展模式相符。

〔7〕参见瑞士卢塞恩大学对贸易协定中电子商务和数字贸易条款数据库的粗略统计，载 https://www.unilu.ch/en/faculties/faculty-of-law/professorships/managing-director-internationalisation/research/taped/#：～：text=The%20TAPED%20dataset%20has%20been%20created%20under%20the，is%20sponsored%20by%20the%20Swiss%20National%20Science%20Foundation，最后访问时间：2022 年 5 月 2 日。

（二）FTA 金融信息传送条款演进

1. 现有 FTA 金融信息传送条款结构演变

FTA 金融信息条款的规则结构演变，分为金融服务规则内单独规制和跨境信息传送一体化规制两个阶段。

第一阶段单独规制以《全面与进步跨太平洋伙伴关系协定》（以下简称为 CPTPP）、《美国—墨西哥—加拿大协定》（以下简称为 USMCA）、RCEP 三大多边 FTA 为代表。《谅解》“信息传送和信息处理”条款确立了“金融信息传送自由原则＋个人数据、个人隐私、个人记录和账户机密性例外”的基础规则结构。CPTPP 金融服务附件的“信息传送”条款在此基础上增加了“基于审慎考虑，要求一金融机构事先获得相关监管机构的授权，以指定一特定企业作为此类信息的接收方”的国家监管权内容。USMCA 金融服务章节的“信息传送”条款将“日常经营所需”限定改为“在许可、授权或注册范围内从事经营”限定，增强了规则明确度，并在实质上进一步增加了国家监管权的内容。但 CPTPP 及 USMCA 均未在“信息传送”条款中明确提及国家监管权，尽管“例外”条款包含“审慎监管例外”，但文本表达限定较多，因而在金融信息传送问题上还是呈现私主体本位的高度自由化理念。

与上述两个美式多边 FTA 不同，RCEP 金融服务附件“信息传送与信息处理”条款转向了国家本位的数据主权理念。该条首先明确了尊重各国国内监管要求的条约立场，其规则结构可以概括为“符合国内法要求的金融信息传送自由”。目前明确列出的两项要求包括传统的“保护个人数据、个人隐私，以及个人记录和账户机密性”及颇受争议的“遵守与数据管理、存储和系统维护、保留在其领土内的记录副本相关的法律和法规”。但从条约解释角度，国家可采取的监管要求并不限于该两项，因此给各缔约国留下了较大空间。究其原因，一方面，RCEP 作为目前全球最大的 FTA，因为各缔约方金融开放程度差异较大，所以在信息传送条款上也呈现出包容性特征。另一方面，以国家传统主权边界为中心的网络主权与数据主权论近年来得到愈来愈多的支持。《中国—东盟关于建立数字经济合作伙伴关系的倡议》提出，“在考察各国法律与社会实际基础上，充分尊重网络主权”，“推动建立多边、民主、透明的全球网络空间命运共同体”。网络主权理论的兴起，在国际政治格局上，以后发国家在网络空间的话语权提升为背景，在当代国际法上，则显示出国家主权在国际社会治理中的绝对核心地位仍不可撼动。在此演化趋势下，网络空间的数据已经转变成为一种战略资源，并将构成一种全新的国家权力要素。〔8〕有学者在对亚太地区的研究中指出：“（信息）国际传送限制在某些方面可以支持国内经济发展，同时也可以作为复杂贸易谈判和地缘政治定位的杠杆。”〔9〕

跨境信息传送一体化规制以 ASDEA 为代表。全球数字竞争格局下，美欧之外的经济体也开始在国际经贸规则变革中发力。ASDEA 将金融信息跨境传送纳入第 23 条“以电子方式跨境传送

〔8〕 See Brad Brown, Michael Chui & James Manyika, Are you Ready for the Era of “Big Data”, 4 *McKinsey Quarterly* 24, 34 (2011)，转引自沈逸：《全球网络空间治理与金砖国家合作》，载《国际观察》2014 年第 4 期。

〔9〕 See Clarisse Girot, Mark Parsons & Olga Ganopolsky, Data Transfers After Schrems II: Reflections from the Asia Pacific, Cross-border Data Forum (Jan. 21, 2021), available at https://www.crossborderdataforum.org/data-transfers-after-schrems-ii-reflections-from-the-asia-pacific/, last visited on May 7, 2022.

信息”条款中统一规制，不再单列。第一，该条首先承认各缔约方对信息传送有其各自的监管要求，融合了国家本位的规制理念。第二，该条以跨境信息传送总体自由为原则（包括个人信息跨境传送自由），同时沿袭了主流“目的限定”而非 USMCA“经营范围限定”的做法。第三，该条对国内监管进行了严格的手段和限度限定：“各国为实现公共政策目标，有权采取或维持与前款要求不一致的措施，但该措施必须：（a）未以构成任意或不合理歧视手段或变相限制贸易的方式实施；以及（b）不会对信息传送施加超过实现目标所需的限制。”不可否认，实际上监管例外能够符合上述所有条件并非易事。〔10〕因此，ASDEA 第一款虽然与 RCEP 表达类似，但效果完全不同，仅是一种调和式的立场宣示。而对于传统的“个人数据、个人隐私，以及个人记录和账户机密性”内容，ASDEA 单列了“个人信息保护”条款进行保护，并将其置于“以电子方式跨境传送信息”条款之前，从而将个人信息保护提高到与跨境信息传送同等地位，不再作为例外事项。

2. 现有 FTA 金融信息传送条款呈现的问题

总体来看，当前诸 FTA 金融服务规则异质化程度高，金融信息传送条款用语不统一，〔11〕规制逻辑也尚未完全梳理清晰，在数据本地化与金融信息传送的关系处理上尤是如此。自 USMCA 在“金融信息传送”条款后一条设置了“计算设施的位置”条款后，USJDTA、ASDEA、《英国—日本全面经济伙伴关系协定》（以下简称为 UKJCEPA）、《合并文本》也都引入了这一规则。计算设施所在地条款可以看作自由主义理念“禁止数据本地化”追求下的规则软化处理，与雷曼兄弟破产案后美国财政部、联邦证券交易委员会等金融监管机构考虑在 FTA 中保留金融数据存储和处理本地化要求的政策空间和美国金融产业界追求数据自由流动利益间的冲突博弈不无相关。〔12〕曾有解读指出，USMCA 的规定与 CPTPP 类似，但未规定可出于审慎考虑要求事先获得监管机构授权，以指定特定信息接收方。〔13〕该观点显然忽视了“金融信息传送”条款与“计算设施所在地”条款的紧密关联，CPTPP 的注释中明确指出：一方可采取或维持不违反本协定的措施，包括符合“例外”条款的任何措施，例如一项措施要求一金融实体事先获得金融监管机构的授权，指定特定企业作为该信息的接收人。但从另一个方面，这也是 FTA 金融信息传送条款逻辑不清的例证。欧盟—澳大利亚、欧盟—新西兰贸易协定谈判中，欧盟提交的初步文本（以下简称为《初步文本》）对此呈现得更为明显：一体化规制趋势下，《初步文本》同样未在“服务与投资”章下的金融服务一节纳入信息传送条款，而在“数字贸易”一章中统一规制，但其“跨境数据流动”条款却以大篇幅阐明禁止本地化要求，根据该条规定，“缔约方承诺确保跨境数据自由流动，以促进数字经济中的贸易”，“为此，双方之间的跨境数据流动不应受到以下限制：a）要求在缔约方境内使用计算设施进行处理，包括强制使用在缔约方境内认证或批

〔10〕 参见马光：《论国际法上网络安全的定义和相关国际规则的制定》，载《中国政法大学学报》2019 年第 3 期。

〔11〕 当前国际层面“数据”与“信息”的内涵差异尚未完全厘清。大部分 FTA 使用“信息传送”作为条款名称，但也存在一些 FTA 使用“数据处理、数据跨境流动”等表述，目前没有条款对金融信息、数据流动或信息传送等用语进行法律界定，不同的用语是否会引起规制范围不同从而使法律效果不同还有待观察。

〔12〕 参见前引〔4〕，杨幸幸文。

〔13〕 参见朱隽：《CPTPP 规则解读之四：金融服务规则》，载微信公众号“国际经济法评论”，2021 年 9 月 22 日。

准的计算设施；b）要求在缔约方境内对数据进行本地化，以便存储或处理；c）禁止在另一方境内储存或加工；d）根据缔约方境内计算设施的使用情况或缔约方境内的本地化要求，进行跨境数据传送”。该条款的逻辑性值得商榷。

三、金融信息传送条款构建的各国路径选择

（一）金融信息传送条款定位

USJDTA、ASDEA 两个数字经济协定对金融信息传送条款的性质及其规则结构进行了重构。传统金融信息传送条款置于金融服务章节，其定性和范围仍然限于“服务”；USJDTA、ASDEA 将金融信息传送纳入数字贸易、数字经济章节，并将范围限于“通过电子手段”，此时金融信息传送不再作为“金融服务”的内容，而是“信息/数据流动”的内容，服务和商品的定性界分被模糊，承诺的范围形式、法律后果都较传统 WTO 语境不同。当前国际社会较普遍地认为数字经济协定是经济联盟的新趋势或新阶段，〔14〕但目前尚缺乏对核心概念的一致定义，不同协定使用的术语及涉及的方面也不同。ASDEA、DEPA 使用“数字经济”，USJDTA、USMCA 使用“数字贸易”，CPTPP、RCEP 则使用“电子商务”。〔15〕此外，在“信息/数据”项下，协定对数据分类和平台类型予以进一步考量，监管中国内各部门间的协调、国家安全和敏感性问题、对文化敏感的解释和适用问题以及国内登记和分类问题也都值得进一步思考。与之相比，《合并文本》和《初步文本》直接将现有信息传送条款的内容合并至电子商务章节的做法则更欠缺逻辑性。UKJCEPA 未改变“金融信息传送”从属于“金融服务”的定性，并将条款名称改为“金融信息”，在其中纳入“金融信息传送自由原则”“个人数据、个人隐私以及个人记录和账户机密性例外”“金融服务计算设施所在地规则”的处理方式是目前为止保守路径下最完善且逻辑自洽的做法。最新 FTA 金融信息传送条款设置情况的对比请参见表 2。

表 2　　最新 FTA 金融信息传送条款设置情况对比

名称	金融信息传送条款设置方式	金融信息传送条款定位
USJDTA	第 5 条审慎例外、货币和汇率政策例外 第 11 条电子方式跨境信息传送 第 13 条金融服务提供者的金融服务计算设施位置 第 15 条个人信息保护	数字贸易章节

〔14〕 See Yaroslav Lissovolik, Digital Economy Agreements: The New Phase in Economic Alliances, Valdai Discussion Club (Feb. 10, 2021), available at https://valdaiclub.com/a/highlights/digital-economy-agreements-the-new-phase/, last visited on May 7, 2022; Shen Yi, Digital Agreements: New Trends in International Alliances, Valdai Discussion Club (Apr. 27, 2021), available at https://valdaiclub.com/a/highlights/digital-agreements-new-trends-in-international-all/, last visited on May 7, 2022.

〔15〕 目前世界上尚无普遍得到认可的电子商务和数字贸易定义，实际上两个概念在多数情况下得以混用。例如，从美国所发起或签订的 FTA 来看，USMCA 之前的 FTA 均采用了“电子商务”的用词，而在 USMCA 中，在内容几乎相同的情况下，“电子商务”章节名称更名为“数字贸易”。参见马光：《国际数字贸易规则的主要议题研究》，载《四川行政学院学报》2020 年第 2 期。

续前表

名称	金融信息传送条款设置方式	金融信息传送条款定位
ASDEA	第 3 条一般例外 第 17 条个人信息保护 第 23 条电子方式跨境信息传送 第 25 条金融服务计算设施位置 第 32 条金融科技与监管科技合作	数字经济章节
UKJCETA	第 8.63 条金融信息 第 8.65 条审慎例外	服务贸易、投资自由化、电子商务章 金融服务分节
《欧盟—英国贸易与合作协定》	第 201 条数据跨境流动 第 202 条个人数据和隐私保护	数字贸易章节
《初步文本》	第 3 条例外 第 5 条数据跨境流动 第 6 条个人数据和隐私保护	数字贸易章节
《合并文本》	第 B.2 条信息流动 (3) 金融信息/金融服务提供者的金融服务计算设施位置	电子商务章节

（二）金融信息传送规制路径差异

1. 美、新、英追求金融信息传送自由化

美国、新加坡、英国在金融信息传送自由化立场上旗帜鲜明，基本都遵循“金融信息传送自由原则＋个人数据、个人隐私、个人记录和账户机密性例外＋严格受限的监管例外＋计算设施本地化规则”的规制逻辑。这与保护本国金融行业进攻利益的需求不谋而合。根据 2021 年 9 月 24 日发布的第 30 版全球金融中心指数报告，纽约在各金融城中位列第一，伦敦位列第二，香港第三，新加坡第四。前 20 中共有 6 座美国城市。〔16〕就英国而言，金融服务业一直是其老牌支柱产业：英国是世界第二大投资管理中心、欧洲最大的保险和长期储蓄提供商，每 14 名英国劳动者中就有 1 人从事金融和相关专业服务工作。英国脱欧后，在金融监管上拥有了更大的自主权和灵活度，并有机会重新审视其数据流动规制方案。2020 年 11 月 9 日，时任英国财政大臣里希·苏纳克在下议院发表声明称希望“恢复英国作为世界卓越金融中心的地位”。〔17〕目前英国政府已经与新加坡达成新的金融服务伙伴关系以确保更大的信息共享，并与美国成立了金融监管工作组，在欧洲经济区国家的金融服务监管中授予了一系列等价保护决定。可以预见，在金融业数字化转型中，美、新、英三国将会有更紧密和深入的合作。

不过，正如前述，尽管都持金融信息传送自由化立场，英国的规制路径又较美新更为保守。从近年签订的 FTA 来看，美新都意图在数字经济领域的规则制定上先发制人，金融信息问题作为数字经济中信息/数据问题的一部分，其所蕴含的国内政策导向是金融领域的全面数字化。也

〔16〕 See The Global Financial Centres Index 30，p. 4.

〔17〕 See Rishi Sunak，A New Chapter for Financial Services，July 2021，available at https://www.gov.uk/government/publications/a-new-chapter-for-financial-services，last visited on May 7，2022.

即，相较于金融业这一国民经济部门，美新都更关注数字经济这一发展模式。而英国目前看来，依旧专注于金融业本身。英式 FTA（UKJCEPA 及英国在 WTO 电子商务谈判中提供的规则文本）在“金融服务计算设施所在地规则”下增加了相当务实的“外部云服务企业同等适用”规则，增加这一规则的背景是英国本土乃至欧洲都缺乏有竞争力的云服务提供者，欧洲企业、公共当局大多采用美国云服务提供者为其提供数据服务。但明确设置“外部云服务企业同等适用”规则也不免传达出这样一种信号：相较于担忧本国缺乏有竞争力的本地云服务提供者，英国更关心如何使本地云服务提供者的缺乏不至影响其跨境金融服务的竞争力。

2. 欧盟在构建数据竞争力目标下的立场变化

与美、新、英不同，欧盟并未对金融领域及金融信息传送特别关注。较早的两个 FTA 中的金融信息传送条款设置完全体现了欧盟在个人权利保护上的突出立场。《欧盟—韩国 FTA》在金融服务分节的“数据处理”条款中特别约定：“各方重申其保护个人基本权利和自由的承诺，应采取适当的保障措施保护隐私，特别是在个人数据传送方面。”并进一步注明，这一承诺所保护的个人基本权利和自由是指《世界人权宣言》、联合国《计算机处理的个人数据文档规范指南》以及 OECD《隐私保护与个人数据跨国流通指南》中规定的权利和自由。《欧盟—加拿大全面经济贸易协定》规定：“各方应有充分的保障措施，以保护隐私，尤其是在个人信息传送方面。如果金融信息的传送涉及个人信息，则此类传送应符合传送发起方所在地区的个人信息保护立法。”欧盟的人权叙事在数据规制议题上抢占了先机，但负面影响也显而易见。一个简单的等式是：数据越多，算法就越智能。对个人数据保护的偏重将不可避免地限制金融机构在经营分析、精准营销等方面的智慧化能力，从而影响欧盟区银行业数字化转型步伐。〔18〕

2020 年，欧盟接连发布《欧洲数据战略》《欧洲数字主权》等文件，以期构建欧洲数字单一市场，维护其全球经济影响力和地缘政治影响力。在《欧洲数据战略》的导向下，欧盟在《欧盟—英国贸易与合作协定》及其他正在谈判的经贸协定中均将跨境数据流动内容统一放到了独立的电子商务章节（过去欧盟 FTA 习惯将电子商务和服务章节放在一起），并从强调个人信息保护转向强调禁止数据本地化。这一转向不可谓不突兀。事实上，施雷姆斯第二案〔19〕后，欧盟内部本地化趋势大大加强，欧洲数据保护委员会于 2020 年 11 月 11 日发布的两份文件《欧洲监督措施基本保证草案》和《补充措施建议》都招致了数据传送规则过于严苛的批评，被认为“将导致严格的数据本地化，给欧盟和美国的企业带来许多重大问题”〔20〕。另外，欧盟委员会于 2020 年 9 月发布的关于《金融部门数字运营弹性监管的草案》区分了在欧盟设立的信息通信技术（以下简称为 ICT）服务提供者和在欧盟没有商业存在的 ICT 服务提供者，并对使用此类第三国 ICT

〔18〕 参见李梦宇：《国际金融业数据治理特征与启示》，载《清华金融评论》2021 年第 5 期。

〔19〕 欧盟法院在本案中认为美国的监控立法违反了《欧盟基本权利宪章》，也没有为欧盟个人提供有效的司法救济，因此欧美之间的“隐私盾”协议无效。详细案件内容可参见 https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en。

〔20〕 Testimony by Peter Swire at the U. S. Senate Commerce Committee Hearing “The Invalidation of the EU-U. S. Privacy Shield and the Future of Transatlantic Data Flows” on December 9, 2020, available at https://www.crossborderdataforum.org/testimony-by-peter-swire-at-the-u-s-senate-commerce-committee-hearing-on-the-invalidation-of-the-eu-u-s-privacy-shield-and-the-future-of-transatlantic-data-flows/, last visited on Nov. 11, 2021.

提供商提出若干限制，如欧盟的金融实体不得使用在欧盟没有商业存在的公司为其提供关键的 ICT 服务。2021 年欧盟各国的数据保护监管机关还启动了多起关于欧盟机构继续使用美国云服务和软件服务是否合法的调查，并暂停了部分合作。虽然欧盟的对外立场不断呈现出向自由化靠拢的趋势，但考虑到数据自由流动将进一步拉大其与美国的数字差距，欧盟似乎正在积极寻求国内监管手段以平衡该等态势。

四、我国立法和 FTA 中金融信息传送规则

（一）确立金融信息传送自由原则

我国在跨境数据流动问题上的立场转向以 2016 年《网络安全法》的出台为分界线。2016 年之前，我国对于跨境数据流动问题关注不多，且对金融监管持绝对审慎态度，2011 年 1 月《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》明确确立了个人金融数据原则上禁止出境的基本方向。2016 年后，尤其是近两年来，随着数据价值的不断凸显，我国内外政策都开始向促进数据自由流动方向发展。国内法层面，《个人信息保护法》《数据安全法》、国家互联网信息办公室《数据出境安全评估办法》已经确立了金融数据“满足数据安全监管要求即可出境”的监管框架。具体到金融相关立法，2020 年修订的《中国人民银行金融消费者权益保护实施办法》（以下简称《实施办法》）删除了原第 33 条对“向境外提供境内个人金融信息”的限制性规定。2020 年《中国人民银行关于发布金融行业标准做好个人金融信息保护技术管理工作的通知》（以下简称《通知》）的附件《个人金融信息保护技术规范》第 7.1.3 条（d）项虽然载明“因业务需要，确需向境外机构（含总公司、母公司或分公司、子公司及其他为完成该业务所必需的关联机构）提供个人金融信息的，应当满足四项具体要求”，但《个人信息保护法》并不禁止关键信息基础设施运营者向境外提供个人信息，且其第 38 条还特别明确“中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行”。因此《个人金融信息保护技术规范》第 7.1.3 条（d）项更应被理解为管理性规范而非对“境外机构”范围的限制性规范。

国际法层面，签署 RCEP、申请加入 CPTPP 已经向全球经济体传达出中国支持金融信息自由传送的立场。实践层面，当前全球数字经济格局中，中美两国参与数字经济并从中受益的能力最强。〔21〕从发展数据来看，在金融服务领域，我国主要金融中心的发展前景良好，且在金融科技指数上表现强劲，但在营商环境上的竞争力并不强。〔22〕在云服务领域，阿里云非常适合处理中国或东南亚客户的云优先数字业务工作负载，有望成为印度尼西亚和马来西亚等新兴云市场所青睐的区域提供商；腾讯云是唯一在俄罗斯拥有业务地域并拥有核心基础设施能力（计算、存储和网络）的超大规模云提供商，而且在网络领域的能力尤为突出。但中国云服务厂商普遍全球发

〔21〕 联合国 2021 年数字经济报告显示，从参与数据驱动的数字经济并从中受益的能力来看，美国和中国脱颖而出。全世界的超大规模数据中心有一半在这两个国家，它们的 5G 普及率最高，它们占过去五年人工智能初创企业融资总额的 94%，占世界顶尖人工智能研究人员的 70%，占全球最大数字平台市值的近 90%。

〔22〕 See The Global Financial Centres Index 30，pp. 8－10.

展动力不足。〔23〕因此，从各个层面来看，确立金融信息传送自由原则都有其现实必要性。

（二）保留必要的金融数据本地化空间

数据本地化与跨境数据流动间的关系一直颇有争议。境内产生的数据在境外云服务器存储必然伴随着数据出境，因此允许境内产生的数据在境外存储即意味着允许跨境数据流动，但反之并不亦然，要求数据在本地存储并不妨碍境内主体将数据传送给境外机构。目前国外学者对数据本地化措施的范围界定还包含保留本地副本等间接或事实的本地化要求，〔24〕进一步增强了数据本地化与数据跨境流动的可切割性。数据本地化要求与数据出境审核等国内监管要求类似，属于边境后措施，而当前各 FTA 除 USMCA 及 ASDEA 外，对跨境金融数据流动自由化的承诺仅覆盖到边境措施。且从现实来看，越来越多的国家和地区正在针对更多的数据类型实施不同程度的本地化政策。从 2017 年到 2021 年，制定数据本地化政策的国家数量从 35 个增加到 62 个，全球数据本地化政策的总数从 67 个增加到 144 个（未包括正在制定的数十个）。其中，采取金融领域数据本地化措施的例子有：（1）卢森堡金融业监管委员会 2012 年 12/552 号通知规定，除非获得明确同意，金融机构必须在卢森堡境内处理数据；（2）2013 年 2 月 21 日俄罗斯银行第 397－P 号条例“关于电子数据库的创建、维护和存储程序”要求所有“信用机构”将所有数据存储在本地；（3）土耳其银行监管局 2020 年发布《银行信息系统条例》，加强了银行和金融服务机构将其主要（实时/生产数据）和次要（备份）信息系统保留在国内的规定；（4）印度证券交易委员会 2020 年发布了一份与网络安全相关的通知，要求金融机构确保对关键系统的完整保护和无缝控制，同时将关键数据保持在印度的法律框架内；（5）韩国 2016 年修订了《电子金融交易监管条例》，允许金融公司使用云服务，但金融服务委员会特别要求在位于韩国的服务器上维护此类数据；（6）智利金融监管机构 2020 年发布了银行业标准的更新汇编，要求在智利保存“重要”或“战略性”外包数据。〔25〕因此，对跨境金融数据流动自由化的承诺今后不可能大范围延及数据本地化禁止，与 ASDEA 类似的对国内监管进行手段和限度限定的做法更有可能成为主流。

我国现行的金融数据本地化要求包括《网络安全法》第 37 条，国务院《征信业管理条例》第 24 条，《保险公司开业验收指引》第三（九）4 条，《通知》的附件《个人金融信息保护技术规范》第 7.1.3 条，中国人民银行《金融数据安全数据生命周期安全规范》第 7.3.2 条等。这些从法律到金融行业标准的规则基本确立了金融数据全面本地化的态度。但《金融数据安全数据生命周期安全规范》同时也指出，1 级数据为公开数据，原则上无保密性要求，2 级数据应优先考虑业务需求，对于非重要数据可以考虑放松本地化要求。

---

〔23〕 See Raj Bala, Bob Gill, Dennis Smith, Kevin Ji & David Wright, Magic Quadrant for Cloud Infrastructure and Platform Services (Jul. 27, 2021), available at https://www.gartner.com/doc/reprints?id=1-271OE4VR&ct=210802&st=sb&_ga=2.98959896.742444110.1644673015-722388850.1644673015, last visited on Feb. 13, 2022.

〔24〕 See James M. Kaplan & Kayvaun Rowshankish, Addressing the Impact of Data Location Regulation in Financial Services (May. 22, 2015), available at https://www.cigionline.org/static/documents/no14_web_0.pdf, last visited on May 7, 2022; IRSG report, How the trend towards data localisation is impacting the financial services sector (December 2020), available at https://www.irsg.co.uk/assets/Reports/IRSG_DATA-REPORT_Localisation.pdf, last visited on May 7, 2022.

〔25〕 See Nigel Cory & Luke Dascoli, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them (Jul. 19, 2021), available at https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost, last visited on May 7, 2022.

（三）规制路径选择

当前，主要经贸协定都转向采取跨境数据流动一体化规制方案。就我国而言，除 2011 年《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》第 6 条外，国内现行各金融相关立法中已无直接规范跨境数据流动的条文。我国在 2021 和 2022 年相继出台了《个人信息保护法》《数据安全法》、国家互联网信息办公室《数据出境安全评估办法》，显示出将数据问题进行统一规制、而非部门化处理的倾向。跨境数据流动一体化规制方案下，数据以个人信息及非个人信息数据划分，而不以具体行业数据划分。在与金融领域类似的领域如工业和信息化领域，工业和信息化部《工业和信息化领域数据安全管理办法（试行）》2022 年征求意见稿删除了 2021 年征求意见稿中“核心数据不得出境”的表述，并增加了“根据国际条约、协定处理外国提供数据请求”及“非经批准不得向外国执法机构提供本地数据”等内容，以与《个人信息保护法》《数据安全法》的规定相统一。目前电信和互联网行业、汽车行业相关数据管理规定/标准也都在制定阶段，其中有关数据出境的内容应当也会与《个人信息保护法》《数据安全法》的规定相统一。另外，与美、新一致，我国的着眼点也在于数字经济这一发展模式，《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》高频次提及全领域数字化，其中当然包括金融机构数字化转型。因此，从国内视角来看，采取跨境数据流动一体化规制方案似乎与我国更为契合。但从条约层面来看，也存在以下问题：第一，现行“数字经济”/“数字贸易”/“电子商务”协定多通过指明“影响通过电子方式交付或提供服务的措施同样需遵守投资及服务章节相关条款所包含的义务”来处理与传统“服务贸易”的范围重叠，但这并未根本解决其在贸易法中的体系定位问题，将金融信息规则并入是否会引起金融开放承诺的扩张尚不可知。第二，各国对一般商贸信息和金融信息的敏感度不同，“数字经济”/“数字贸易”/“电子商务”协定中的信息传送条款通常较金融服务章节更为严格，如 CPTPP 即对电子商务章节“通过电子方式跨境传送信息”条款下缔约方可采取的例外措施施加了手段和限度限制，而金融服务章节的“信息的传送”条款未设置此等限制。第三，各国在“数字经济”/“数字贸易”/“电子商务”上分歧明显，从名称到具体内容，如数据本地化、源代码等问题，都存在较大谈判难度。

因此，从实践角度，将金融信息传送条款保留在金融服务章节更有利于现阶段的条约谈判；而将信息传送问题统一置入数字经济协定与我国的规制方向更为契合，但承诺的水平无疑将更高，国内法与国际法的统筹难度也将更高。总体而言，FTA 金融信息传送规则构建上应当注意以下几个问题：第一，协调我国金融服务开放承诺水平与金融信息传送自由化水平，如采取跨境数据流动一体化规制方案，则应考虑增加与 RCEP 中“任何规定不得解释为要求一缔约方允许与其未作出承诺相关的跨境提供或者境外消费服务”类似的条款。第二，应当明确（金融）信息传送规则不适用于由一缔约方或以其名义持有或处理的信息，或与该信息有关的措施，包括与收集信息有关的措施，并增加在数据获取上的司法、执法合作。第三，保留金融领域的保密性要求，即任何规定不得解释为要求一缔约方披露与个人客户相关的事务和账户信息，或公共实体拥有的任何机密或专有信息。第四，可考虑接受对国内监管例外进行一定的手段和限度限定。“金融业是一个高度全球化的体系，金融机构的跨境支付清算、客户尽职调查、国际化运营、全球信息技

术系统集成、集团化风险管理与境外信息报送等，都离不开数据跨境。”〔26〕除明晰的法律指引之外，加强数据合规服务行业建设，从而降低境内外金融服务商的合规难度，同样是扩大金融开放、融入全球金融市场的关键步骤。在具体监管方案运用方面，依赖数据和技术的智能监管、有效的内控信息披露、成熟的行业标准自律和健全的合同执行制度或也将为更有效的数据监管提供有益指引。

五、结　语

“一国在自由贸易协定下的话语权体现为该国在谈判过程中制定规则的权力，并服务于该国的政治经济利益。法律输出正是大国实现自由贸易协定制度控制以实现其话语权的一种路径。”〔27〕20 世纪末以来，美国与欧盟成功依靠 FTA 输出了国内规范和核心价值理念，《服务贸易协定》谈判的坎坷则充分显示了两大话语权掌控者之间的冲突。在今天，中国也应当积极考虑通过法律输出路径提高自身在国际贸易的话语权，以期实现从国际秩序遵守者向国际规则制定者的转变。同时，可以看到，FTA 金融信息传送条款并不是一个孤立的规则，在文本上，它与电子商务规则、个人信息保护规则、审慎例外规则、本地化规则相交织，在规制理论上，对其的考量应当从跨境数据流动议题，甚至网络空间治理的全局角度出发，构建框架完整、逻辑统一的理论体系。

2022 年初欧盟委员会发布《欧盟标准化战略——制定全球标准，支持弹性、绿色和数字化的欧盟单一市场》提出：“标准是欧盟单一市场和全球竞争力的无声基础，在标准化活动中拥有一个强大的全球足迹，并在关键的国际论坛和机构中领导工作，对于欧盟保持全球标准制定者的地位至关重要。通过制定全球标准，欧盟可以输出其价值观，同时为欧盟公司提供重要的先发优势。”〔28〕“欧盟及其成员国必须在国际电信联盟、国际标准化组织和国际电工委员会以及其他相关的全球伙伴关系、论坛和联盟中，推动对国际标准化活动采取更具战略性的方针，以确保欧盟的全球竞争力、安全和开放的战略自主权，以及欧盟推广其价值观的能力。”〔29〕数字全球化背景下，数字标准是贯穿各种经济活动过程的隐形基础。在金融领域，我国金融标准化技术委员会公布的金融国际标准（截至 2021 年 9 月 30 日）为 66 项，国家标准（截至 2021 年 12 月 13 日）为 83 项。随着数字化发展和进一步深入开放，标准的数量将大幅增加，各科技企业在国际标准制定中的参与度也将提高。此外，根据国际惯例，国际金融合作一般也适用《新巴塞尔协定》、国

〔26〕 李伟：《我国金融数据跨境流动规则建设的思考与建议》，载《中国银行业》2020 年第 1 期，第 42 页。

〔27〕 王燕：《自由贸易协定下的话语权与法律输出研究》，载《政治与法律》2017 年第 1 期，第 109 页。

〔28〕 New approach to enable global leadership of EU standards promoting values and a resilient, green and digital Single Market (Feb. 2, 2022), available at https://ec.europa.eu/growth/news/new-approach-enable-global-leadership-eu-standards-promoting-values-and-resilient-green-and-digital-2022-02-02_en#:~:text=New%20approach%20to%20enable%20global%20leadership%20of%20EU,within%20the%20Single%20Market%20as%20well%20as%20globally, last visited on May 8, 2022.

〔29〕 Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions-An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market, p. 5.

际证监会组织标准、国际保险监督官协会标准等国际金融协议和监管标准。〔30〕而我国目前在标准领域尚不发达，普遍来看，大多数中国公司都缺乏一种结构化和战略性的标准化方法，以捕捉其与各种经济运营的相关性，无论是法律合规性、市场准入还是一般商业战略。同时，随着如人工智能、数据保护或网络安全等新领域的衍生，对于标准制定能力的挑战将更大。培养标准化专家、深入国际标准制定或许是一个可以提升我国话语权的路径。

Abstract: Under the framework of international trade law, transfer of financial information clause constitutes the core part of financial information transfer rules. Originated from Transfers of Information and Processing of Information clause in Understanding on Commitments in Financial Services which was appended to the Final Act of the Uruguay Round, transfer of financial information clause was subsequently adopted by numerous FTAs. With digital economy upsurge, attention to the regulation of cross-border data flows began to focus on e-commerce and digital trade. As a result, there is a trend to integrate transfer of financial information clause into cross-border information transfer provisions of e-commerce or digital trade in FTA in recent years. However, there are still many fundamental issues to be resolved in the integrated regulation approach, and should be viewed with caution. At the present stage, transfer of financial information clause have developed a basic structure of "freedom of financial information transfer as principle + personal data, personal privacy and the confidentiality of individual records and accounts exception + limited regulatory exception" and rules on the "location of financial services computing facilities" have been derived from the issue of data localization. China should upgrade the FTA financial information transfer rules on the basis of its position on data sovereignty and shift from being an international rule-taker to an international rule-maker, with a view to safeguarding its offensive interests in the financial services and digital technology sectors.

Key Words: cross-border data flows, financial information transfer, FTA transfer of financial information clause, financial data exit

（责任编辑：肖　芳　赵建蕊）

〔30〕 参见云倩：《“一带一路”倡议下中国—东盟金融合作的路径探析》，载《亚太经济》2019 年第 5 期。

财经法学 No. 1，2022
pp. 3 - 17

信息主体同意的适用边界

李群涛　高富平*

内容提要：在欠缺其他合法性基础情形下，信息主体同意是否适用，关键在于处理的个人信息是否含直接标识符。直接标识符能单独表征信息主体身份，从而使信息处理风险与信息主体身份精准连结。因此，出于尊重陌生人社会信息主体隐匿身份的自由、尊重信息主体对处理风险的自主决策，信息主体可以通过同意控制含直接标识符的个人信息，即“单独识别个人信息”。但同意不适用于“结合识别个人信息”。首先，结合识别个人信息具有模糊性，个人信息处理者难以就此直接识别信息主体身份进而征求同意。其次，《个人信息保护法》确立了处理结合识别个人信息不需告知规则，逻辑上也要求有相应的不需同意规则。最后，结合识别个人信息不适用同意规则也是实现“促进个人信息合理利用”这一立法目的的可行路径。

关键词：单独识别个人信息　结合识别个人信息　同意　直接标识符　个人信息保护法

一、引　言

《民法典》与《个人信息保护法》已经相继出台，作为个人信息保护制度重要内容的同意规则，其框架已经建构完成。无论《民法典》第1035条第1款第1项还是《个人信息保护法》第13条第1款第1项，都确认“信息主体同意”这一合法性基础的重要地位。然而在解释上尚未明确之问题为：当不具备《个人信息保护法》第13条第1款第2至7项所列举的合法性基础时，〔1〕信息主体同意是否适用于对各类个人信息的处理行为。此即本文尝试回答的信息主体同意之适用边界问题。

针对信息主体同意之适用边界问题，学界已有讨论，并形成四种学说。按照各学说主张的适

* 李群涛，华东政法大学法律学院博士研究生；高富平，华东政法大学法律学院教授。

〔1〕 关于《个人信息保护法》第13条所列七项合法性基础的研究，参见程啸、王苑：《论个人信息处理中无需取得个人同意的情形》，载《人民司法》2021年第22期。

用范围从小到大排列，分别为“无适用空间说”“敏感个人信息说”“全部个人信息说”和“全部个人信息＋匿名信息说”。笔者逐一简要述评。

“无适用空间说”认为，同意规则不能适用于任何个人信息之上，甚至不宜作为个人信息处理的合法性基础。〔2〕然而，《民法典》和《个人信息保护法》仍然坚守同意规则，故该说不为现行法所接纳。

“敏感个人信息说”认为，同意规则仅适用于敏感个人信息。〔3〕然而目前同意规则位于《个人信息保护法》“个人信息处理规则”章的“一般规定”中，该制度的体系位置至少表明一般个人信息并非一概不适用同意规则。故该说亦不为现行法所接纳。

“全部个人信息说”认为，同意规则适用于全部个人信息。〔4〕当然该说亦承认应当针对不同类别个人信息建构一套宽严有别的梯度保护体系。〔5〕该说似符合法条文义，但不利于实现《个人信息保护法》所确立的“促进个人信息合理利用”的立法目的。笔者将于本文第三、四部分详细论证，此处不赘。

“全部个人信息＋匿名信息说”认为，同意规则适用于现行《个人信息保护法》中规定的个人信息与匿名信息。〔6〕然而无论《网络安全法》第 42 条第 1 款但书，还是《民法典》第 1038 条第 1 款但书，抑或《个人信息保护法》第 4 条第 1 款皆明定匿名信息不适用同意规则。因此，该说亦不为现行法所采。

综上，关于信息主体同意的适用边界问题，上述四说均难谓妥当。

个人信息是与个人有关的各种信息，同意是个人信息处理的合法性基础，个人信息处理者为取得同意，在收集个人信息之前即需判断信息主体身份。然而个人信息范围无边无界，大量个人信息在信息主体身份判断方面具有模糊性，这对个人信息处理者于处理前履行“取得同意义务”造成障碍。

于是，本文提出，按照是否含直接标识符的标准将个人信息划分为“单独识别个人信息”与“结合识别个人信息”，同意规则仅适用于单独识别个人信息。事实上此种对个人信息的分类方法在学界的讨论中并不少见，〔7〕甚至已经为现行法所接纳（《民法典》第 1034 条第 2 款），但是鲜有观点将此种分类与同意规则的适用边界相联系并进行证成。〔8〕本文首先勾勒该边界的轮廓，

〔2〕 参见任龙龙：《论同意不是个人信息处理的正当性基础》，载《政治与法律》2016 年第 1 期。

〔3〕 参见汤敏：《论同意在个人信息处理中的作用——基于个人敏感信息和个人一般信息二维视角》，载《天府新论》2018 年第 2 期。

〔4〕 参见陆青：《个人信息保护中“同意”规则的规范构造》，载《武汉大学学报（哲学社会科学版）》2019 年第 5 期；徐丽枝：《个人信息处理中同意原则适用的困境与破解思路》，载《图书情报知识》2017 年第 1 期。

〔5〕 参见丁晓强：《个人数据保护中同意规则的“扬”与“抑”——卡－梅框架视域下的规则配置研究》，载《法学评论》2020 年第 4 期。

〔6〕 参见林洹民：《个人信息保护中知情同意原则的困境与出路》，载《北京航空航天大学学报（社会科学版）》2018 年第 3 期。有必要指出，该说否认存在匿名信息，因为技术界人士已经明确表示不存在绝对不可复原的匿名信息。在此基础上，按照该说，仅当法律规定了不准复原义务时，现行法所述的匿名信息才豁免适用同意规则。

〔7〕 参见陶盈：《我国网络信息化进程中新型个人信息的合理利用与法律规制》，载《山东大学学报（哲学社会科学版）》2016 年第 2 期。

〔8〕 有学者曾提及此方面，但并未展开。参见胡文华、黄道丽、孔华锋：《个人数据保护“同意规则”的检视及修正》，载《计算机应用与软件》2018 年第 9 期。

进而分别论证同意适用于单独识别个人信息，而不适用于结合识别个人信息。

二、信息主体同意规则适用的判断标准：含直接标识符

信息主体同意是否适用，其判断标准就在于个人信息是否含有直接标识符。在重视和重新界定直接标识符概念的基础上，个人信息分为单独识别个人信息与结合识别个人信息。

（一）直接标识符概念的重视与重新界定

直接标识符是指能够单独识别特定自然人身份的信息。〔9〕直接标识符的典型特征在于具有唯一性〔10〕和身份指向性，例如身份证号、社会保险号码、人脸信息等。需要注意的是，直接标识符与特定自然人是单向唯一对应关系。具言之，一直接标识符只对应唯一特定自然人，但一特定自然人将有许多直接标识符。所谓身份指向性意味着存在直接标识符即足以识别信息主体真实身份。正如学者所言，信息的人格属性集中体现在其可识别特定自然人身份的性质。〔11〕

我国立法已经接纳了直接标识符概念。我国个人信息概念借鉴欧美，而这一来源于欧美的概念恰恰无法脱离直接标识符。例如，欧盟《一般数据保护条例》（GDPR）第 4 条 a 项后半句中的身份证号等系本文所述直接标识符。同样地，美国立法一直强调直接识别符（direct-identifier）概念作为个人可识别信息（PII）的重要判断标准。与这一国际趋势相一致，我国实质上已经接受直接标识符概念，《网络安全法》第 76 条第 5 项以及《民法典》第 1034 条第 2 款，都具体列举了不少直接标识符，如身份证号码、生物识别信息等。

直接标识符可谓信息主体风险的重要来源。现代社会是风险社会，技术应用确实会给人类带来一定风险。同样地，在个人信息领域，大数据技术应用可能导致风险产生。然而，如果风险产生无法对应特定身份、不会影响到特定自然人，那么对于该自然人而言这或许并非风险，即使是也不必过于关注和担忧。但如前所述，直接标识符的本质特征在于其唯一性和身份指向性，直接标识符恰恰使个人信息处理者可知晓特定自然人身份。直接标识符在个人信息中具有重要地位，个人信息与个人身份的勾连往往依赖直接标识符。个人信息处理风险主要在于风险能通过个人信息直接传导至具有特定身份的自然人，此中起桥梁作用者正是直接标识符。

随着时代发展，直接标识符的范围已日渐扩张。目前，直接标识符包括社会身份标识符和生物身份标识符，后者是对传统直接标识符概念的扩张。〔12〕以前，直接标识符主要指身份证号、驾照号码、护照号码、社会保险号码、军官证号、工作证号、出入证号、社保卡号、居住证号码等社会身份标识符。〔13〕生物身份标识符后来也成为直接标识符的重要来源。例如，随着人脸识别技术发展，人脸信息等与特定信息主体之间也形成了唯一对应和身份指向关系。总之，某符号

〔9〕 参见《中国互联网定向广告用户信息保护行业框架标准》。

〔10〕 参见范姜真媺：《大数据时代下个人资料范围之再检讨——以日本为借镜》，载《东吴法律学报》2017 年第 2 期。

〔11〕 参见刘士国：《信息控制权法理与我国个人信息保护立法》，载《政法论坛》2021 年第 6 期。

〔12〕 参见《信息安全技术个人信息安全规范》（GB/T 35273—2020），附录 A，第 23 页；上海市地方标准《数据去标识化共享指南》（DB31/T 1311—2021）。

〔13〕 参见《信息安全技术个人信息安全规范》（GB/T 35273—2020）之附录。

具有唯一性和身份指向性，即可被认定为直接标识符。

直接标识符与间接标识符、准标识符均非同一概念。一方面，直接标识符与间接标识符并非同一概念。如果仅就“唯一性”而言，手机等智能设备序列号（又称“国际移动设备识别码”，简称 IMEI）也具有唯一性。仅依此虽能触及个人但不能识别个人身份，因此不具有前述直接标识符的“身份指向性”特征。于是，本文称之为“间接标识符”。另一方面，直接标识符与准标识符亦非同一概念，两者差异为是否具有唯一性。美欧都有实质意义上的准标识符概念。美国的准标识符（quasi-identifier）〔14〕对应欧盟 GDPR 第 4 条 a 项中的“个人属性”（factors），包括民族、种族、婚姻状况、身体、心理、基因、精神状态、经济、文化、社会因素等。准标识符中的“准”（quasi）字表明其本质上并非标识符。一个准标识符可能会对应多位自然人，不具有唯一性。例如，“研究生”是准标识符，能够对应千千万万研究生，无法指向特定自然人身份。

（二）基于直接标识符对个人信息的区分

以是否含有直接标识符为标准可将个人信息周延地分为单独识别个人信息和结合识别个人信息。

1. 单独识别个人信息

以前对个人信息相当部分的讨论恰以单独识别个人信息为基本思考模型。事实上 20 世纪即已经产生个人信息保护问题，当时个人信息即以单独识别个人信息为主。例如：“姓名张三，性别男，年龄 65 岁，身份证号 123456789012345678，电话号码 12345678901，家庭住址青海省西宁市湟源县胜利镇未来街道幸福小区 1 栋 1 单元 1025 号，银行卡号……”此为含有直接标识符个人信息（即单独识别个人信息）的典型样态。个人信息处理者据此能直接了解此个人信息对应的信息主体身份。单独识别个人信息的典型特征即在于含直接标识符。就此而言，《民法典》第 1034 条第 2 款中的“能够单独识别特定自然人的信息”与《个人信息保护法》第 4 条第 1 款中的“与已识别的自然人有关的各种信息”可表达同一含义。正因如此，本文一律用“单独识别个人信息”指代含直接标识符的个人信息。

单独识别个人信息，强调信息“含”直接标识符，而非除直接标识符之外没有其他信息。换言之，一旦数据集中含有直接标识符，直接标识符与其后跟随的购物记录、行踪轨迹等结合组成单独识别个人信息。如上所述，随着时代发展，直接标识符的概念有所扩张，生物身份标识符即为直接标识符的最新内容。因此，单独识别个人信息之范围亦相应扩张，兹不赘述。另外，是否“含”直接标识符，应当以数据集为单位全面审视，而非割裂个别数据项而单独看待。就此而言，直接标识符有可能是由一个数据集中多个数据项共同组成的，例如，在一个含有姓名、性别、学校、班级、行踪轨迹等数据项的数据集中，姓名、性别、学校、班级将共同构成直接标识符。

〔14〕 也有译为“间接标识符”，但须指出，此间接标识符与本文所谓间接标识符并非同一含义。参见刘颖、谷佳琪：《个人信息去身份化及其制度构建》，载《学术研究》2020 年第 12 期；程海玲：《个人信息匿名化处理法律标准探究》，载《科技与法律》2021 年第 3 期。

2. 结合识别个人信息

与单独识别个人信息相对的是结合识别个人信息，即不含直接标识符的个人信息。《民法典》第1034条第2款中“能够与其他信息结合识别特定自然人的各种信息”以及《个人信息保护法》第4条第1款中“与可识别的自然人有关的各种信息”，描述的均为不含直接标识符的个人信息。为表统一，本文一律用“结合识别个人信息”的概念。

结合识别个人信息也属于个人信息的范畴，但在未与直接标识符相结合的情况下，仅凭结合识别个人信息难以识别身份。换言之，信息主体以外的人仅通过结合识别个人信息来识别个人身份是需要成本的。目前个人信息定义无限扩张，这几乎成为国际社会的共识。欧盟第29条工作组出台的关于个人信息概念的意见对个人信息概念明显采广义理解，强调与其他信息结合能识别自然人身份或者特征，以及综合考虑内容、目的和影响三因素的情况下与个人有关系。〔15〕甚至按照欧洲学者分析，天气信息有时也能成为个人信息。〔16〕经扩张后的个人信息概念，其判断标准已经从能识别身份变为相关处理行为对人（不一定为特定自然人）有风险的信息。〔17〕按照《个人信息保护法》第4条第1款对个人信息的定义，我国接受了此种扩张标准。此标准非以信息当下状态为观察视角，而是要求立足当下预测充满无限可能之未来，即以未来看现在，这使得个人信息边界显著扩张且趋于模糊。从此角度而言，信息即使不含直接标识符，亦不妨碍被认定为个人信息从而适用个人信息保护相关规则。

结合识别个人信息大致有两类来源：一是各类传感器设备所收集的个人信息；二是从原始处理者或其他处理者处间接获取的经去标识化处理的信息。一方面，随着传感器的广泛布设，智能穿戴设备、网络设备的普及以及物联网技术的飞速发展与充分应用，海量的个人相关信息被快速采集供给、实时加工分析。但是相应地，部分传感器等设备能做到的只是实时记录个人有关情况而无法提供个人直接标识符等信息（信息主体主动提供的除外）。另一方面，随着信息实践不断开展，部分主体所控制的信息已经是经去标识化处理的信息。

需要注意结合识别个人信息与匿名信息的关系。所谓匿名信息是指经处理无法识别个人且不能复原的信息（《个人信息保护法》第73条第4项）。匿名信息制度通行于欧美而非我国独创。欧盟GDPR“鉴于条款”（recital）第26段明确指出，匿名信息（anonymous information）不适用于该法。该段同时指出，为了确定自然人是否可识别，应当考虑个人信息处理者或其他人（by another person）的识别能力，因此，匿名信息意味着任何人都无法通过匿名信息识别自然人身份。简言之，欧盟规定的匿名信息客观上不具有识别可能性。不过有专家已经声明，技术方面“匿名化是一种幻想”，只能达到识别可能性比较低的水平。〔18〕美国法学会2020年公布《数据隐私法律原则重述》，并在第2条中指出，无法识别个人的（non-identifiable）信息不适用数据隐私

〔15〕 See Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN WP 136.

〔16〕 See Nadezhda Purtova, The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law, 10 *Law, Innovation and Technology*, 40 (2018).

〔17〕 参见范为：《大数据时代个人信息保护的路径重构》，载《环球法律评论》2016年第5期。

〔18〕 See Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 *UCLA Law Review*, 1701 (2010). 当然，由此观之欧盟规定的匿名信息认定标准并不合理，对此本文不再详述。

保护原则。〔19〕不同的是，欧盟匿名信息指客观上无识别可能性，而美国“无法识别的个人信息”是指识别可能性极低。然而此种无法识别的个人信息仍具有一定的识别可能性，如果不使其受制于个人信息保护规范，那么将使该部分信息暴露于风险之中。为了弥补这一点，美国的匿名信息制度有其预设前提，即禁止再识别。〔20〕或许是受欧美影响，我国《个人信息保护法》第 4 条第 1 款规定匿名信息不属于个人信息。然而借鉴比较法的重要前提是我国与借鉴对象有相同的制度环境。〔21〕我国《个人信息保护法》第 73 条第 4 项没有明确规定禁止再识别要求，且在难存此解释空间的情况下，一旦将我国匿名信息等同于美国无法识别的个人信息，将导致对匿名信息的处理失去控制。而且从笔者梳理的 50 多个法域的法律文本来看，极少有对个人信息定义作如此限制的先例。但《个人信息保护法》既已作如此规定，只能认为应对匿名信息进行严格把握，当无法确定是否满足客观“不能复原”要件时，应当认定该信息为结合识别个人信息而非匿名信息。

三、同意规则适用于单独识别个人信息

信息主体能够以同意来控制个人信息的处理行为，其正当性基础在于由宪法上的个人尊严、自由以及主体地位推演而得的个人事务自决。〔22〕笔者以下欲指出，在个人信息领域，个人事务自决主要体现为尊重陌生人社会个人隐匿身份的选择和自由，以及尊重信息主体对处理风险的决策。此二理由均仅指向单独识别个人信息。

（一）尊重陌生人社会个人隐匿身份的自由

现代社会是陌生人社会，〔23〕隐匿身份是陌生人社会中的个人选择和自由。〔24〕人口增加、人口流动性增大和社会不安全因素混杂，导致公众轻易不愿意暴露身份。虽然社会交往要求社会中每个人必须允许其他人了解自己，但是此种要求也应仅限于与个人有交往关系之人。例如，一个人的亲朋好友、同事、老师、同学、交易对手，甚至欲与其缔结合同者。但不应无限扩展到千里之外与个人毫无瓜葛的陌生人。逐渐地，是否隐匿身份成为个人自主决定的事项，受到社会认可和法律保护。

〔19〕 See The American Law Institute, Principles of the law-Data Privacy (2020), available at https://1.next.westlaw.com/Document/I0f02ee65145811eb8a02f30620293de0/View/FullText.html?ppcid=1c4fd268d6b54fc98b7f1ebff22c23f3&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=%28sc.Search%29, last visited on Dec. 3. 2021.

〔20〕 按照美国《数据隐私法律原则重述》(2020) 的总结，其所谓不适用数据隐私法律原则的匿名信息条件有三：第一，采用合理方法去掉个人信息上的标识符；第二，使去标识符后的个人数据处于较低风险水平；第三，个人信息处理者不再重新识别个人。

〔21〕 参见〔德〕茨威格特、克茨：《比较法总论》(上)，潘汉典等译，中国法制出版社 2014 年版，第 30 页。

〔22〕 参见田野：《大数据时代知情同意原则的困境与出路——以生物资料库的个人信息保护为例》，载《法制与社会发展》2018 年第 6 期；王雪乔：《论欧盟 GDPR 中个人数据保护与“同意”细分》，载《政法论丛》2019 年第 4 期；高富平：《同意≠授权——个人信息处理的核心问题辨析》，载《探索与争鸣》2021 年第 4 期。

〔23〕 近年来已经有相关文件关注到陌生人社会这一社会转型现象。参见《东莞市人民政府办公室关于印发〈东莞市深化“二标四实”工作总体方案〉的通知》(东府办〔2018〕44 号)；《江苏省民政厅对省十三届人大一次会议第 5015 号建议的答复》。学理上的讨论，参见张清、王露：《陌生人社会与法治构建论略》，载《法商研究》2008 年第 5 期；龚长宇、郑杭生：《陌生人社会秩序的价值基础》，载《科学社会主义》2011 年第 1 期；何绍辉：《论陌生人社会的治理：中国经验的表达》，载《求索》2012 年第 12 期。

〔24〕 参见龚长宇：《陌生人社会：价值基础与社会治理》，中国人民大学出版社 2021 年版，第 105 页。

然而，处理单独识别个人信息，将侵犯个人自主决定是否隐匿身份的自由。单独识别个人信息处理强调获得个人同意，其背后价值观与陌生人社会伦理基础不可分割。有学者称，“个体对于个人隐私和个人信息的身份识别的保护就是基于传统熟人环境社会下的潜在人格尊严和人格自由意识，而人们对于识别性的风险和恐惧多来自于传统观念下的身份泄露”〔25〕。显然，这种保护身份意识蔓延到了陌生人社会，成为个人典型的自由。如果毫不相干的主体欲全面了解一陌生人的单独识别个人信息（事实上就是了解身份），那么实在无任何正当性可言。虽然许多学者提及将分散的个人信息汇聚成大数据对于发挥数据经济价值、促进公共福利具有重大意义，但是直接标识符并非达致该目标所利用的大数据之必需。难以想象无任何交往关系的陌生私主体为了促进公共利益，需要利用他人之个人信息而且非含直接标识符不可。笔者强调，本文讨论的前提是不存在《个人信息保护法》第 13 条第 1 款第 2—7 项合法性基础，故为紧急救助而处理个人信息的情形不在本文讨论范围。正因如此，有学者指出，二次利用个人信息的首要条件是脱敏，即除去直接标识符。〔26〕简言之，陌生人可以收集他人的个人信息甚至进行个性特征分析，但是不允许其擅自知晓该“他人”的真实身份。社会学学者将这种秩序称为对陌生人“冷漠的尊重”。〔27〕

只有获得特定信息主体同意，才能使个人信息处理者与特定信息主体之间的显名交往正当化。在陌生人社会中，应然社会秩序是尊重他人的不同观念和不同选择。每个人相对于他人皆为“道德异乡人”，抱有不同信念、恪守不同行为规范；仅当取得他人“允许”“同意”“包容”时才能达成双方间新的共同行为规范。〔28〕陌生人社会的价值观在于每个人仅允许与其有关系的人了解其个人身份（当然随着关系远近了解程度会有不同），没有社会关系的陌生人不能了解其个人身份。与此相对应，允许与特定个人没有社会关系的人收集、使用该特定个人的个人信息，但仅限于收集、使用结合识别个人信息且不得在分析特征的过程中分析出真实身份。这便是个人信息领域陌生人的行为规范。如果处理单独识别个人信息，则等同于突破陌生人之间行为规范，因此，只有获得信息主体的同意以形成双方间新共同行为规范时，处理单独识别个人信息才被允许。或许出于类似考虑，有学者也指出信息主体能够支配自己的姓名、身份证号码、相貌特征等等。〔29〕此观点值得赞同。

（二）尊重信息主体对处理风险的决策

直接标识符的存在使得信息处理风险得以精准传导至具有特定身份的自然人。“风险可以被界定为系统地处理现代化自身引致的危险和不安全感的方式。”〔30〕如直接标识符定义所阐释，其最大特征为与特定自然人身份具有唯一对应性。个人信息处理者通过其所控制的单独识别个人信

〔25〕 苏今：《〈民法总则〉中个人信息的“可识别性”特征及其规范路径》，载《大连理工大学学报（社会科学版）》2020 年第 1 期，第 86 页。

〔26〕 参见姬蕾蕾：《论个人信息利用中同意要件的规范重塑》，载《图书馆》2018 年第 12 期。

〔27〕 参见前引〔24〕，龚长宇书，第 19 页。

〔28〕 参见前引〔24〕，龚长宇书，第 115－116 页。

〔29〕 参见郭明龙：《论个人信息之商品化》，载《法学论坛》2012 年第 6 期；韩强：《人格权确认与构造的法律依据》，载《中国法学》2015 年第 3 期。

〔30〕〔德〕乌尔里希·贝克：《风险社会》，何博闻译，译林出版社 2004 年版，第 19 页。

息便能直接识别信息主体而不需要进行任何处理行为（识别行为）。对此类单独识别个人信息进行分析，其决策结果可以通过直接标识符的桥梁作用精准配置于特定自然人。此种结果对于特定自然人而言可能有好有坏。例如，银行处理特定自然人单独识别个人信息用以评估该特定自然人信用情况，当处理结果符合信用要求时对该自然人而言有正向反馈，但当处理结果不符合信贷政策所要求的信用等级时，对于该自然人而言具有不利影响，因为这将关系到信息主体是否能顺利申请贷款。但算法不同以及其他因素，导致处理分析行为结果是好是坏无确定性甚至不可预期，这本身对于信息主体而言即为一种风险。除此之外，此类个人信息的滥用以及被篡改、毁损、丢失等都是对信息主体的风险。从《居民身份证法》《统计法》《刑法》等条文来看，我国个人信息立法的重要目的恰是为维护自然人人身、财产安全免受威胁。〔31〕

既然直接标识符的存在客观上产生了个人信息处理的风险与信息主体身份连结的效果，那么出于个人事务自决，应当允许个人对其未来风险进行自主判断和决定。尤其是当个人信息处理者从信息主体处直接收集个人信息时，双方处于直接交互状态，同意机制落实也较为简单。〔32〕如果立法者倾向于剥夺个人判断决策资格而一律允许个人信息处理者处理此类个人信息，那么即剥夺了个人自主决定、自主判断空间，此为典型的法律父爱主义，〔33〕将使信息主体暴露于个人信息处理的风险之中。即使法律对个人信息处理者行为进行规范和要求，也不能保证个人信息处理者必然严格遵守规则，此即禁止性规定会配套法律责任条款的重要原因。不仅如此，即便个人信息处理者遵守各类规定，也不见得处理行为不产生任何风险。当然，允许信息主体自行决策，原理在于允许个人对于精准连结身份的未来风险进行判断和决策，而非出于个人对其个人信息的完全控制。〔34〕关于该点，有学者通过细致考究已经指出，目前广为流传的个人信息自决权是对德国人口普查案的以讹传讹，〔35〕所以此处信息主体同意是个人自治的具体体现，是个人事务自决的应有之义。

事实上，避免存在直接标识符而导致信息处理风险精准传导至个人，亦符合国际个人信息保护制度的基本逻辑。以下以具有代表性的美国和欧盟的制度分别说明。

美国的信息主体同意规则重点关注可识别个人信息（personally identifiable information，简称 PII），即本文所述单独识别个人信息。起初按照美国的隐私控制理论，信息主体有资格决定个人信息在何时、以何种程度和方式进行流动。〔36〕但是隐私控制理论与美国人的信息自由信仰背道而驰。此种情况下，为了缓和信息控制和流动之间的张力，美国通过《儿童网络隐私法》等一系列法案将信息主体对个人信息的控制限制在 PII 范围内，即处理 PII 要经过信息主体同意，而 PII 恰恰相当于本文的单独识别个人信息。虽然美国分散式个人信息保护立法使 PII 的边界动态变化，但美国人的信息主体仅控制 PII 的立场却始终坚定。甚至根据美国最新出台的《统一个人

〔31〕 参见高富平：《个人信息保护立法研究》，光明日报出版社 2021 年版，第 195 页。

〔32〕 参见前引〔8〕，胡文华等文。

〔33〕 参见孙笑侠、郭春镇：《法律父爱主义在中国的适用》，载《中国社会科学》2006 年第 1 期。

〔34〕 关于该问题的讨论，参见前引〔22〕，王雪乔文；张勇：《APP 个人信息的刑法保护：以知情同意为视角》，载《法学》2020 年第 8 期；前引〔11〕，刘士国文。

〔35〕 参见杨芳：《个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体》，载《比较法研究》2015 年第6 期。

〔36〕 See Alan F. Westin，Privacy and Freedom，25 *Washington and Lee Law Review*，166 (1968).

数据保护法》（The Uniform Personal Data Protection Act，简称 UPDPA）〔37〕第 7 条第 b 款第 5 项结合同条第 a 款第 1 句，可以得出结论：针对去直接标识符的个人信息进行处理不需要获得信息主体的同意。〔38〕例如，在针对群体的医学研究中，为了研究某种疾病的地域分布关系，在收集各地患者数据时，至多同时收集患者所在省、市、县即可，没有必要得知患者姓名、身份证号等数据项，甚至患者的精确地址亦不具有必要性。此时个人信息处理者便不需要取得信息主体的同意。由是观之，美国人基本认为若无 PII 则不存在权益威胁。

欧盟的制度也体现了类似的思路。欧盟 2016 年制定了 GDPR，2018 年正式生效执行。部分关于 GDPR 的研究表明同意规则将赋予信息主体对其个人信息的超强控制力。〔39〕但在 GDPR 尚未生效执行的 2017 年，欧盟第 108 号公约协商委员会就出台了《大数据社会个人数据处理中的个人保护指南》。〔40〕其中指出，“大数据应用的复杂性和模糊性应该促使规则制定者不再将控制概念局限于个人控制（个人信息）。他们应该（将控制个人信息概念）理解为更广义的控制个人信息使用”〔41〕。显然欧盟欲澄清，信息主体同意对其个人信息的控制范围远不及研究者所言之广泛。

因此，为尊重陌生人社会个人隐匿身份的自由，尊重信息主体对处理风险的决策，信息主体同意适用于单独识别个人信息。

四、同意规则不适用于结合识别个人信息

基于尊重信息主体对处理风险的决策，以及尊重陌生人社会个人隐匿身份的自由，可以得出同意适用于单独识别个人信息的结论。基于此二者，同样能够从反面佐证同意不适用于结合识别个人信息。不仅如此，本部分另从避免《个人信息保护法》两套识别标准的“基因缺陷”、避免同意规则与不需告知规则衔接不畅，以及避免“促进个人信息合理利用”的立法目的不达三个角度证明，同意规则不适用于结合识别个人信息。

---

〔37〕《统一个人数据保护法》系由美国统一法律委员会制定，于 2021 年 7 月通过的示范法案，拟于 2022 年 1 月前后实施，该法案载于 https://uniformlaws.org/committees/community-home/librarydocuments/viewdocument?DocumentKey=afdb7812-a7c6-4468-92f6-fac09416c0ac。

〔38〕根据 UPDPA 第 7 条第 b 款第 5 项，对于创建假名或匿名化数据具有合理必要性的处理行为，是兼容的数据处理行为。根据 UPDPA 第 7 条第 a 款第 1 句，控制者或处理者可以在未经数据主体同意的情况下从事兼容的数据处理行为。因此，根据 UPDPA 第 7 条第 b 款第 5 项结合同条第 a 款第 1 句，对于创建假名或匿名化数据具有合理必要性的处理行为，不需要取得数据主体的同意。以举重以明轻的法学原理对该项规定深入研究可得出以下结论：创建假名化数据的行为针对的是能单独、直接识别数据主体的个人数据，该行为尚且不需要取得数据主体的同意，则假名化完成后的数据不能单独、直接识别数据主体，对该类数据的处理行为更不需要获得数据主体的同意。UPDPA 中的假名化数据为去除直接标识符的个人数据，大致相当于本文所指“结合识别个人信息”。

〔39〕参见王成：《个人信息民法保护的模式选择》，载《中国社会科学》2019 年第 6 期。

〔40〕Guidelines on the Protection of Individuals With Regard to the Processing of Personal Data in a World of Big Data, available at https://ccdcoe.org/uploads/2019/09/CoE-170123_Guidelines-on-protection-of-individuals-with-regard-to-processing-of-personal-data-in-a-world-f-big-data.pd, last visited on Dec. 3, 2021.

〔41〕《大数据社会个人数据处理中的个人保护指南》，李群涛译，高富平校，载 http://www.dataprotection.cn/news/126.html，最后访问时间：2021 年 8 月 30 日。

（一）避免个保法两套识别标准的“基因缺陷”

认定个人信息时，采较为宽松的识别可能性标准，个人信息处理者本身是否具有直接识别能力，在所不问；然而取得同意却恰以个人信息处理者本身具有直接识别能力为前提。两者所持标准差异导致同意规则不能及于全部个人信息，特别是不适用于结合识别个人信息。〔42〕

个人信息认定环节的判断标准是客观识别标准，其要求“个人信息处理者或者其他任何人”有能力根据信息识别信息主体身份，不仅限于个人信息处理者自身有此识别能力。单独识别个人信息是个人信息中最为典型的一类。然而，随着世界各国认识到个人信息处理活动涉及信息主体利益甚巨，出于加强信息主体权益保护目的，个人信息保护法适用范围相应扩张。〔43〕作为个人信息保护法适用门槛，个人信息范围也需随之扩张。于是国际上普遍认可，若个人信息处理者不能通过信息单独识别信息主体，而是结合其他信息可以间接识别，那么该信息（结合识别个人信息）亦属于个人信息。不仅如此，在欧盟 GDPR 影响下，国际社会进一步认同：即使个人信息处理者不能通过信息识别个人，而其他任何人（by another person）具有此种识别能力，那么该信息也属于个人信息。至此，作为个人信息判断重要标准的识别，已经从特定个人信息处理者能够识别，扩张到世界上（至少是个人信息处理者活动范围内）任何其他人能够识别。此观点被欧盟第 29 条工作组严格贯彻，〔44〕欧洲法院也在相应判决中落实这一标准。〔45〕以至于欧洲学者嗟叹，个人信息保护法某种程度上已成为“万物之法”。〔46〕简言之，为了保护个人权益，已经以当前世界上先进识别技术和丰富信息量为标准（客观识别标准）判断特定信息是否为个人信息。

然而就同意规则而言，履行“取得同意”义务必然以主观识别标准——特定个人信息处理者的实际识别能力（甚至是直接识别能力）——为限。取得同意义务是个人信息处理者自身需要履行的义务，依照“法律不强人所难”的基本法理，个人信息处理者履行某义务必然要以有履行此义务的能力为限。个人信息处理者履行取得同意义务要以信息中含有直接标识符为限，此系同意的时间要求所致。按照《个人信息保护法》第 13 条第 1 款第 1 项规定，取得信息主体同意的，个人信息处理者方可处理个人信息。易言之，原则上取得同意应当先于处理行为进行方为合法。而结合其他信息进行间接身份识别也是处理行为，因此，同意也应当先于间接识别行为而进行，否则违法。同意这一时间要求，迫使个人信息处理者在取得同意之前不得以处

〔42〕 See Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *The EU General Data Protection Regulation (GDPR) A Commentary*, Oxford University Press, 2020, p. 395.

〔43〕 两份个人信息保护领域的重要文件引领了对信息主体的强保护，分别是世界经济合作与发展组织发布的《隐私保护与个人数据跨境流通指南》和欧洲理事会发布的《个人数据自动化处理中的个人保护公约》。此二文件成为之后各国立法的重要参照文件。

〔44〕 参见前引〔15〕，Article 29 Data Protection Working Party 文。

〔45〕 See Case T－670/16, Digital Rights Ireland v. European Commission, GC, order of 22 November 2017 (ECLI: EU: T: 2017: 838); Case C－434/16, Peter Nowak v. Data Protection Commissioner, judgment of 20 December 2017 (ECLI: EU: C: 2017: 994); Case C－345/17, Proceedings brought by Sergejs Buivids, judgment of 14 February 2019 (ECLI: EU: C: 2019: 122); Case C－40/17, Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV., judgment of 29 July 2019 (ECLI: EU: C: 2019: 629).

〔46〕 参见前引〔16〕，Nadezhda Purtova 文，第 78 页。

理的方式进行识别。因此，同意方面的合规，要求个人信息处理者必须在取得同意之前能单独、直接识别信息主体的身份。个人信息认定环节的客观识别标准与同意规则中的主观识别标准间的差距，使得同意控制范围注定无法及于各类个人信息上的处理行为。有学者将客观标准概括为“识别可能性”（identifiability），而将主观识别标准概括为“识别本身”（identification），并指出同意规则仅关注后者，即识别本身。〔47〕两种识别标准只有在面对单独识别个人信息时才重合。揣测普遍漠视这一差距的原因，或许是个人信息保护制度研究基本以 APP 从信息主体处直接采集个人信息的场景作为典型思考模型。于是，收集、存储、分析个人信息，当然不存在不知信息主体身份的情形。此亦从侧面说明，同意规则适用范围的限缩，往往起因于个人信息处理者非从信息主体处直接收集个人信息情形（即俗称的“个人信息二手利用”）的广泛存在。总之，个人信息的外延比同意规则所能适用的个人信息外延大得多，超出的部分包括特定个人信息处理者能够结合识别出身份的个人信息以及特定个人信息处理者本身不能结合识别出身份的个人信息。

两标准范围的不完全重合，恰恰是由于个人信息认定环节“识别”标准的极大扩张为个人信息保护制度创设的“基因缺陷”。由此观之，对个人信息范围采广义理解的国家，只要其采选进机制（opt-in），即取得同意应先于处理行为进行，则其个人信息保护体系中的同意规则亦需限缩于单独识别个人信息。欧盟发现了这一基因缺陷，并通过设置 GDPR 第 11 条试图进行解决。根据该条，个人信息处理者〔48〕有时不必仅为了合规而获取信息主体同意。也正因如此，欧洲学者赞扬 GDPR 第 11 条称，该条“弥合了（至少是试图弥合）由个人信息概念引发的鸿沟”〔49〕。

（二）避免同意规则与不需告知规则衔接不畅

同意不适用于结合识别个人信息，即要求针对结合识别个人信息建立“不需同意”制度。此系对《个人信息保护法》“不需告知”制度的必要呼应。

《个人信息保护法》设立了不需告知规则。《个人信息保护法》第 18 条第 1 款为“不需告知”制度提供了依据。“不需告知”制度主要适用于三种情形：第一，信息主体已经知情，不再需要告知；第二，已经公开的个人信息，不再需要告知；〔50〕第三，当个人信息处理者客观不识别身份或基于合规要求不被允许识别身份时，基于法律不强人所难的基本法理，也应当作为前述不需要告知情形之一。GDPR 有类似制度，其第 13、14 条分别针对从信息主体处收集个人信息、非从信息主体处收集个人信息两种情形规定了告知义务的例外情形。尤其是第 14 条第 5 款 b 项提出，个人信息处理者提供相应信息被证明是不可能或者需要投入过多不必要精力时，个人信息处理者不需要告知。不过，GDPR 亦非完美：根据 GDPR 第 11 条第 2 款，当个人信息处理者的处

〔47〕 参见前引〔42〕，Christopher Kuner 等书，第 395 页。

〔48〕 GDPR 与我国《个人信息保护法》在术语使用上略有不同。GDPR 的数据控制者对应我国的个人信息处理者。GDPR 的数据主体，对应我国的个人，即本文所谓信息主体。术语上的不统一将导致文本阅读上的障碍，为避免这一问题，本文在介绍 GDPR 条文时一律使用我国的术语。

〔49〕 前引〔42〕，Christopher Kuner 等书，第 395 页。

〔50〕 参见程啸：《论个人信息处理者的告知义务》，载《上海政法学院学报（法治论丛）》2021 年第 5 期。

理目的不要求识别信息主体身份，且个人信息处理者能够证明自己无法识别信息主体时，如果个人信息处理者可以（if possible），则需要履行告知义务。然而当个人信息处理者不能识别信息主体时，个人信息处理者如何能够履行告知义务。于是，欧洲学者亦无奈表示，只能依赖“如果可能的话”（if possible）这一条件弥补第 11 条第 2 款的缺憾。〔51〕换言之，一般宜认为此种情况下告知义务无履行可能。

因为告知是取得同意的前提和要求，所以不需告知规则应配以不需同意制度。按照《个人信息保护法》第 14 条第 1 款第 1 句，同意应当在信息主体充分知情的前提下作出。但当信息主体不知情时（此为常态），个人信息处理者必然需通过告知使其充分知情。是故，在逻辑上告知、知情、同意依次发生，通常情况下告知是同意的逻辑前提。“告知同意”或者“知情同意”这一学界和实务界通用且公认的提法事实上已经表明告知是同意的逻辑前提。〔52〕既然如此，那么由于客观或者合规等原因不能告知信息主体时，当然也就无法取得信息主体的同意。这就要求《个人信息保护法》有对应不需告知规则的不需同意制度。

然而《个人信息保护法》没有同步设计不需同意制度。我国虽然设计了不需告知规则，但显然同意规则与此不相适应，因为按照第 13 条规定的文义，当无其他合法性基础时，各类个人信息的处理都需要以获得信息主体同意为前提，其他因素在所不问（此亦为本文引言中“全部个人信息说”的依据）。从全国人大相关机构在立法过程中形成的一系列有关欧盟个人信息保护制度和美国隐私保护制度的研究材料，以及《个人信息保护法》众多条文的表述观之，我国《个人信息保护法》立法明显有参考 GDPR 的现象。然而仅就告知同意规则来看，我国并未做到全面、完整、正确地进行制度参考。上文已经提及，我国不需告知规则学习了 GDPR 第 13、14 条，但对应此种情形，GDPR 配套设置了第 11 条第 1 款不需同意规则，即如果个人信息处理者处理个人信息的目的不要求或不再要求识别信息主体身份，则不应强制个人信息处理者仅为合规而保留、获取或处理额外信息以识别信息主体身份。言下之意，当个人信息处理者不需识别身份时，其处理不需要取得同意。但是我国只吸收了不需告知规则，没有同步建立作为其逻辑后果的不需同意制度。

当然，GDPR 第 11 条第 1 款并非我国不需同意制度的最佳选择。相反，GDPR 第 11 条第 1 款本身存在严重的逻辑漏洞，此处简要分析。根据欧盟 GDPR 第 11 条第 1 款可推知，若处理之目的不要求识别信息主体身份，则以识别身份为前提的同意也不需要获得。简言之，根据该条，是否要求获得同意系以“是否需要识别身份”为根本判断标准。需要识别信息主体身份，则需要获得同意，反之则不需要。看似周延的结论掩盖了逻辑上的漏洞，此处逻辑上的漏洞主要是指遗漏考虑一种情形，即处理结合识别个人信息（即不含直接标识符的个人信息）且处理目的要求识别信息主体身份。根据 GDPR 第 11 条第 1 款，此种情形，由于“需要识别”所以需要获得同意。

〔51〕 参见前引〔42〕，Christopher Kuner 等书，第 396 页。

〔52〕 参见前引〔17〕，范为文；叶名怡：《论个人信息权的基本范畴》，载《清华法学》2018 年第 5 期；前引〔22〕，田野文；王利明：《数据共享与个人信息保护》，载《现代法学》2019 年第 1 期；张新宝：《个人信息收集：告知同意原则适用的限制》，载《比较法研究》2019 年第 6 期；万方：《隐私政策中的告知同意原则及其异化》，载《法律科学（西北政法大学学报）》2019 年第 2 期；吕炳斌：《个人信息保护的“同意”困境及其出路》，载《法商研究》2021 年第 2 期。

然而只有通过“识别身份”这一处理行为识别出信息主体身份才能得到其同意，而同意只能为同意之后的处理行为提供合法性基础，不能为同意之前的识别身份行为及其之前行为提供合法性基础。因此笔者指出的这种情况，根据 GDPR 第 11 条第 1 款，识别出身份之前阶段的处理行为必然将因无合法性基础而违法。法律不强人所难，所以识别身份及其之前的行为也不应当要求获得个人同意。因此，GDPR 以“是否需要识别”作为划分同意适用边界的标准并不合理，应当以是否含有直接标识符（无需进行处理即可识别身份）作为划分标准。我国没有移植 GDPR 第 11 条第 1 款，一定意义上避免了陷入前述逻辑漏洞，但这不能表明我国不应该设立不需同意制度。

于是，我国应建立的不需同意制度，不能盲目追随 GDPR，而是应基于《个人信息保护法》条文，在解释上将单独识别个人信息作为同意规则的适用范围，而将结合识别个人信息排除于同意规则适用范围之外。如前所述，我国应当存在不需同意制度。但显然，我国法缺失这一制度，导致同意规则与告知规则衔接不畅。而《个人信息保护法》生效后，必须从解释论层面寻找新出路。此即需在现行法框架下基于解释论提出具有相同功能的替代方案。而本文所提出的同意适用边界限缩恰恰是解释论下的一种有效解决方案。同意适用边界限于单独识别个人信息，并非意味着结合识别个人信息将不受控制，只是说明结合识别个人信息将不受信息主体的事前控制。但基于法律规定产生的个人信息处理者义务仍然继续适用，《个人信息保护法》规定的事前个人信息保护影响评估等措施仍然应当落实，以保护信息主体权益。并且，此时应当对个人信息处理者课以更高要求。〔53〕

（三）避免个人信息流通利用的立法目的不达

确认结合识别个人信息的处理不需要同意，恰恰能激励个人信息处理者将个人信息处理活动维持于低风险状态。个人信息保护的本意是平衡个人信息处理利用与个人信息处理利用过程中信息主体权益维护。当个人信息已经为结合识别个人信息时，已经使个人信息处理活动处于低风险水平。如果仍然认为结合识别个人信息之处理亦须取得信息主体的同意，那么必然以重新识别信息主体身份为前提，则反而因为合规要求使得个人信息重新被暴露于高风险环境。〔54〕最终与个人信息保护法立法目的相悖。正是因为单独识别个人信息与结合识别个人信息的风险水平有异，所以对两者不应采相同保护水平。结合识别个人信息之处理不需要个人同意，是对此类信息处理的制度激励，有利于鼓励个人信息处理者积极主动地对个人信息进行去标识化处理。事实上，《个人信息保护法》本身也将去标识化作为安全技术措施（第 51 条第 3 项）。

《个人信息保护法》的重要目的之一在于“促进个人信息合理利用”。信息是自由的，个人信息亦未完全脱离自由的本质，只是因为个人信息以个人为主题，所以属于特殊信息类型，需要一定程度的特殊对待。而结合识别个人信息，多属于用以分析个性特征的信息，这些信息只

〔53〕 参见前引〔42〕，Christopher Kuner 等书，第 447 页。

〔54〕 See Paul M. Schwartz，Daniel J. Solove，The PII Problem：Privacy and a New Concept of Personally Identifiable Information，86 *New York University Law Review*，1814 (2011).

有与特定个人身份关联起来，可以直接通过该信息识别信息主体身份时，才涉及隐私等人格利益问题，这意味着鼓励在不危及信息主体权益情形下对结合识别个人信息进行分析利用。当然，若导致不利后果，那么可以通过民事侵权救济而非事前控制机制，保证信息主体权益得到保护。现行法已经建立起这样的事后救济机制。当信息主体权益遭受侵害或有受侵害之虞但尚未造成损害时，《民法典》第 1037 条等已经提供了各类防御性人格权益请求权。〔55〕当信息主体权益遭受侵害并造成损害时，《个人信息保护法》第 69 条第 1 款确立了专门的损害赔偿制度。

不过，需要强调，结合识别个人信息与单独识别个人信息可能互相转换，一旦结合识别个人信息转化为单独识别个人信息，则又需要适用同意规则。处理结合识别个人信息不必获得同意，甚至连分析行为也不必获得同意。但是一旦通过处理行为识别到信息主体身份，结合识别个人信息瞬间转换为单独识别个人信息，于是应当立即寻求信息主体的同意。此时一旦同意没有取得，那么根据《个人信息保护法》第 47 条第 1 款，个人信息处理者应当删除所涉个人信息。某种意义上，结合识别个人信息转换为单独识别个人信息的时刻，很可能是个人信息处理者删除个人信息的时刻。

五、结　语

“保护个人信息权益”与“促进个人信息合理利用”是《个人信息保护法》第 1 条确立的同等重要的立法目的。该法给法律解释适用者提出的艰巨任务是实现两个目的的和谐与平衡。然而，若认为缺失《个人信息保护法》第 13 条第 1 款第 2 至 7 项的合法性基础时，对各类个人信息的处理都要经过同意，那么天平上的砝码已经过于向保护个人信息权益一侧倾斜。划定同意规则的适用范围正是“瞻前顾后”地通盘考虑两种目标的平衡之后在同意规则上的体现。本文主张信息主体的同意只能适用于对单独识别个人信息的处理行为。此结论在法律解释上体现为应当对《民法典》第 1035 条第 1 款第 1 项主文中的“自然人”以及《个人信息保护法》第 13 条第 1 款第 1 项中“个人”概念进行限缩，限缩至“个人信息中以直接标识符直接体现其身份的个人”。当然，个人信息处理的合法性须从目的合法、具有合法性基础，以及处理行为规范三个方面综合甄别。本文讨论的同意边界问题仅是合法性基础方面判断的问题，不涉及目的是否合法和处理行为是否规范两方面。

使结合识别个人信息摆脱信息主体同意的控制，也正是在法律上为目前国家提倡的数据流通机制提供法律基础。2020 年 3 月公布的《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》提出加快数据要素市场建设，其内含的要求便是为数据流通创造法律上的途径。个人信息是数据中的重要类别，当然应该考虑其流通利用的合法性问题。但目前个人信息流通机制于法律方面的困境在于逐一获取信息主体的同意，合规成本极大。本文试图为结合识别个

〔55〕 参见高富平、李群涛：《个人信息主体权利的性质和行使规范——〈民法典〉第 1037 条的解释论展开》，载《上海政法学院学报（法治论丛）》2020 年第 6 期。

人信息未经信息主体同意而流通利用的可行性提供法理支撑，以便在一定程度上为个人信息的流通利用松绑。

Abstract：In the absence of other legal basis，the key to the applicability of personal information subject's consent lies in whether the personal information contains a direct identifier. The direct identifier can directly represent the identity of the personal information subject，so as to accurately link the information processing risk with the personal identity. In addition，in the stranger society，the choice and freedom of individual hiding identity should be respected. Therefore，the direct identifier representing identity information should be controlled by the personal information subject，that is，applicable boundary of personal information subject's consent is individually identifiable personal information. However，consent does not apply to personal information without direct identifier. Firstly，as the fuzziness of this kind of personal information，it is difficult for personal information processors to directly identify the subject of personal information and ask for consent. Secondly，logically，the non disclosure system established by the personal information protection law needs the non consent system. Finally，the non application of consent system is also the important way to achieve the legislative purpose of personal information circulation and utilization.

Key Words：individually identifiable personal information，personal information without direct identifier，agree，direct identifier，personal information protection law

（责任编辑：武　腾　赵建蕊）

财经法学 No. 3，2022
pp. 80 - 95

论信息主体的知情同意及其实现

常宇豪*

内容提要：知情同意是各国个人信息保护法普遍采用的基本规则，也是我国个人信息保护法律的核心规则。知情同意制度的法理基础来源于对信息主体意思自治的保障，通过充分告知后的有效同意实现信息主体对其个人信息的自主控制。大数据时代，随着个人信息来源的多元化和二次利用的广泛化，知情同意正面临隐私政策晦涩冗长、信息主体知识匮乏、信息处理者强制“二选一”、新型个人信息处理行为难以适用知情同意、频繁知情同意导致的告知疲劳等一系列困境。鉴于知情同意的重要价值和在个人信息保护制度中的基石性地位，轻言放弃并非明智之举。应采取多元共治模式，通过信息处理者依法告知、信息主体增强知情能力和行权意识、公共机构完善法律制度和严格执法司法、社会组织强化行业自律和第三方认证等举措，保证信息主体知情同意的实现。

关键词：个人信息　意思自治　知情同意困境　多元共治

一、问题的提出

知情同意是个人信息保护法的基石和核心制度，也是个人信息自主控制的实现途径和处理个人信息的合法性基础。该制度肇始于1973年美国健康、教育和福利部报告（HEW报告）中提出的“公平信息实践原则”（FIPPS）。美国、日本等国家和欧盟、经合组织（OECD）等国际组织均将知情同意作为个人信息收集、使用的重要合法性基础，并建立了“告知—同意”（Notice/Consent）框架保证制度实施。受国际立法尤其是同属于成文法域的欧盟法影响，我国也将“告

* 常宇豪，西南政法大学经济法学院博士研究生。

本文为国家社科基金重点项目“创新社会治理背景下社会企业法律规制研究”（18AFX018）、国家社科基金项目“网络金融消费者个人信息保护研究”（17BFX096）的阶段性成果。

知—同意”确立为个人信息保护的基础性规则。2021年1月1日开始实施的《中华人民共和国民法典》和11月1日正式实施的《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）均将“告知—同意”确定为个人信息处理的核心规则。《个人信息保护法》更进一步将知情权和同意权确认为信息主体在个人信息处理过程中的权利，开启了个人信息法律保护的新篇章。〔1〕

然而，与立法中不断强化的趋势相悖，现实中的知情同意却面临着功能式微甚至可能被架空的危险。一方面，由于告知文本不友好、信息主体缺乏知情主动性等原因，信息主体“告而不知”，同意的有效性遭到质疑；另一方面，不加区分的适用知情同意形成巨大的经济和社会成本，限制了大数据产业发展和社会整体福利提升。如何克服知情同意的现实困境，弥合制度建构与法律实践之间的鸿沟，使知情同意真正成为信息主体自主控制、自我保护之良方和个人信息处理的“总阀门”，成为《个人信息保护法》实施亟待解决的重大问题。基于此，本文以《个人信息保护法》解释论为视角，在分析知情同意的规范内涵和制度价值基础上，针对其存在的现实困境提出解决策略，为《个人信息保护法》的实施提供智识支持。

二、知情同意的规范内涵与制度价值

（一）同意的法理基础：意思自治

探究知情同意的规范内涵和制度价值，逻辑上应以其法理基础为依归。在历史上，“同意”一直发挥着认可他人行为的作用，“同意被认为是与他人‘有同样意向的状态’，被认为表达了一种‘心理上的赞成态度’或表明情感与意见方面的一致”〔2〕。洛克在《政府论》中提出“一切自然人都是自由的，除了他自己同意以外，无论什么事情都不能使他受制于任何世俗的权力”〔3〕。这是“同意”首次被赋予法哲学上的意义。可见，“同意”概念在被引入法学领域之初就与意思自治存在紧密联系。

由于个人信息和信息主体存在密切关联，信息处理者在收集使用个人信息时告知信息主体并获得其同意，是信息主体对个人信息控制和支配的体现。有学者即指出“同意证明了个人权利的存在”〔4〕。意思自治赋予了自然人根据自己的自由意志设立、变更、终止民事法律关系的权利，信息主体可以自由决定是否许可他人收集、处理、利用自己的个人信息。“同意”则是意思自治在个人信息保护中的实现机制和外在体现。在信息处理者收集信息主体的个人信息并进行加工利用而形成的法律关系中，信息主体享受信息处理者通过收集、利用个人信息提供的高质量服务，同时其对个人信息的支配权受到一定限制。在这一过程中，个人利益在不同方面出现了增益和减损，如何平衡这种增减进而使个人利益最大化即体现了每个个体的意思自治。信息主体可以选择“同意”信息处理者收集、利用个人信息的请求以换取大数据时代的种种便利，也可以选择“不

〔1〕《个人信息保护法》第44条规定：“个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。”

〔2〕 John Kleinig，The Ethics of Consent，8（12）*Canadian Journal of Philosophy*，91－118（1982）.

〔3〕〔英〕洛克：《政府论》（下篇），叶启芳、瞿菊农译，商务印书馆1964年版，第74页。

〔4〕 George P. Fletcher，*Basic Concepts of Legal Thought*，Oxford University Press，1996，p. 109.

同意”放弃分享数据红利以保证个人信息的安全。民事主体在自由、理性选择行为方式的同时，对于所选择的行为方式引发的后果，无论好坏，皆应自己承担。〔5〕欧盟数据保护第二十九条工作组（Article 29 Data Protection Working Party）也在意见书中指出：“自由作出的同意意味着某个具有正常能力的人在不受任何胁迫（无论是社会的、经济的、心理上的或其他种类的）的情况下所作出的自愿的决定。”〔6〕同时，信息主体的“同意”也使信息处理者获得了收集、利用个人信息的正当性。

信息主体同意作为个人信息处理中的基本原则具有法理和制度设计上的双重基础。在法理维度，“同意”体现了法律对个人根据自己意思自由决定自身事务的承认，是对人格尊严和主体性的尊重。洛克认为：“人是自己的主人，是自身和自身行动或劳动的所有者。”〔7〕在美国法律语境下，借以保护个人信息的隐私权被认为是“对个人私生活领域的管控”〔8〕。可见，个人有权决定自己的私人事务，其中显然包含了个人信息。一个人在其基本权利行使的正当范围内，若缺乏自治自决的机会，将丧失尊严，因此，自决权应受到国家及他人之尊重。〔9〕在法律规范维度，同意是在信息主体和信息处理者的事实不平等关系中，保护信息主体权利的一种制度设计。在信息主体与信息处理者的互动中，信息主体处于不可逆转的劣势地位。在此种情形下，基于理性人假设，将保护自己信息的权利赋予信息主体就成为最有效的选择。事实上，同意原则也的确是基于“假设几乎所有的人，在所有时候，做出的选择都是基于自己的利益最大化，或者至少比其他人为自己做出选择好很多的考虑”设计的。〔10〕由信息主体控制自己的个人信息并独立决定是否允许信息处理者收集、使用，使得信息主体拥有了对抗处于强势地位的信息处理者的筹码。一方面，信息处理者为使用个人信息必须承诺妥善保护信息主体的个人信息，并与信息主体分享利用个人信息带来的利益；另一方面，信息处理者的这种承诺事实上也成为信息主体维护自身信息权益的依据。因此有学者指出：“在个人和信息处理者的不对等关系中，权利人同意是一个最好的制约性权利。同意是个人对抗信息处理者的唯一对话途径，反映了信息处理者与个人的互动过程。”〔11〕

（二）有效同意的条件：知情、自愿、明确作出

既然同意关乎个人的意思自治和利益维护，同意的有效性就至为重要。那么，何种同意方为有效，其条件为何？只有厘清此问题，才能探知知情同意的规范内涵。根据《个人信息保护法》第 14 条第 1 款“基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出”之规定，我国法上的有效同意应当具备充分知情、自愿做出、明确表示三个基本条件。其中，“知情”是有效同意的基础和前提。按照《现代汉语词典》的解释，知情是对某件事

〔5〕 参见谭启平：《中国民法学》，法律出版社 2015 年版，第 55 页。

〔6〕 Article 29 Data Protection Working Party, Working Document on the Processing of Personal Data relating to Health in Electronic Health Records (EHR), Feb. 15, 2005, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf, last visited on Jan. 24, 2022.

〔7〕 前引〔3〕，洛克书，第 28 页。

〔8〕 谢远扬：《信息论视角下个人信息的价值——兼对隐私权保护模式的检讨》，载《清华法学》2015 年第 3 期，第 100 页。

〔9〕 参见李震山：《从生命权与自决权之关系论生前预嘱与安宁照护之法律问题》，载《中正大学法学集刊》1999 年第 2 期。

〔10〕 See Richard H. Thaler, Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness*, Yale University Press, 2008, p. 9.

〔11〕 徐丽枝：《个人信息处理中同意原则适用的困境与破解思路》，载《图书情报知识》2017 年第 1 期，第 110 页。

情原委情状的了解，充分知情自然是对该事情的充分了解。只有在对个人信息处理相关情况充分了解的前提下，信息主体的同意才能体现自己的个人意志。“自愿”是信息主体做出决定时的状态，即信息主体必须是在无任何胁迫、欺诈或威胁状态下做出的同意决定。“明确”则是同意的外在表现形式，要求同意是明确、不含糊的肯定行为。我国法的这一规定与欧盟《关于涉及个人数据处理中的个人保护以及此类数据自由流动的第 95/46/EC 号指令》（以下简称《95 指令》）、《一般数据保护条例》（General Data Protection Regulation，简称 GDPR）中的“同意”基本一致。按照 GDPR 第 4 条第 11 款之规定，“数据主体的‘同意’是指数据主体依照其意愿自愿作出的（freely given）、具体的/特定的（specific）、知情的（informed）及明确的（unambiguous）确认意思表示。通过声明或明确肯定的行为做出的这种意思表示，表明其同意对其相关的个人数据进行处理。”〔12〕但与欧盟法四要素不同的是，我国法并未将“具体的/特定的”（specific）作为限定条件。根据“欧盟数据保护第二十九条工作组关于同意的指南”（Guidelines on Consent under Regulation 2016/679）的解释，“具体的/特定的”要素包含两层含义：（1）个人信息处理的目的需要具体、特定，初始目的之外的个人信息处理行为，需要重新获得同意，此规定意在约束超预期目的处理行为；（2）同意请求事项需要与其他信息区隔，每个同意请求必须提供独立的信息，相应的同意必须是针对特定事项的，此要素意在防止捆绑请求、概括同意。〔13〕需要指出的是，尽管我国《个人信息保护法》未将“具体/特定”要素作为有效同意的必要条件，但“单独同意”制度的设置与此有异曲同工之效。

个人信息领域对于有效同意条件的规定有深厚的哲学基础和实践基础。约翰·克莱尼格（John Kleining）在其《同意的伦理学》中将“同意”界定为“一个人倾向于便利他人的主动性行为，并且同意的主体要在这一便利中承担责任”〔14〕。即同意可以被理解成是一种个人与他人“交互作用”的行为。这种主客体之间交互作用的“同意行为”必须满足三个条件，即同意必须是自愿地（voluntarily）、知情地（knowingly）以及故意地/专门地（intentionally）做出的。同意的这三个特征共同保证了同意的真实性（genuineness），只有完全满足以上三个条件的主动性同意行为才能被认为是有证成效力的真实的（genuine）同意，而只有真实的同意才是人们真实意愿的表达。〔15〕因此，作为哲学意义上的“同意”，“知情”便成为其基础和前提。从行为逻辑学的视角看，同意是对他人意见、主张或者请求事项的赞同、准许，而赞同、准许等肯定性行为是对他人意见、主张或者请求事项全面了解、知情并做出理性判断的结果，因此，有效同意的基础必然是充分知情，不知情的同意则为无效同意。

医疗领域是知情同意研究最久、理念最成熟的领域，为个人信息保护中知情同意制度的设计奠定了实践基础。为了体现知情对患者做出同意决定的重要性，早在 1948 年《纽伦堡法典》就提出了“自愿同意”法则。〔16〕它指出：“自愿同意是指有关人员在法律上有资格提供同意；并应

〔12〕《欧盟〈一般数据保护条例〉GDPR（汉英对照）》，瑞栢律师事务所译，法律出版社 2018 年版，第 43 页。

〔13〕See Article 29 Data Protection Working Party，Guidelines on Consent under Regulation 2016/679，p. 16.

〔14〕前引〔2〕，John Kleinig 文，第 91 页。

〔15〕参见刘笑言：《同意的困境——基于以同意理论证成政府家长式干预的视角》，载《北京航空航天大学学报（哲学社会科学版）》2011 年第 3 期。

〔16〕参见马特：《民事视域下知情同意权的权利基础及规则建构》，载《江淮论坛》2014 年第 5 期。

处于能行使自由选择权利的境况下，而没有暴力、欺骗、欺诈、强迫、哄骗以及其他隐蔽形式的强制与强迫等因素干预；应该对所涉及的问题有充分的知识和领会，使他能够理解并作出明智的决定。”并且，法典还以“自愿”“法律上有行为能力”“理解”和“知情”四个要素来说明自愿同意。〔17〕法典将研究参与者的“知情”作为自愿同意的重要基础，同时将行为能力、理解能力和知识储备等保证参与者能充分知情的前提条件置于重要位置，足以表明知情对同意决定的重要性。纽伦堡审判之后，知情同意逐渐成为医患关系中，特别是人体试验领域最受关注的原则之一。〔18〕知情同意规则的建立标志着在医疗领域“知情”作为有效“同意”的基础性地位得以确立。鉴于“知情”对有效同意的重要性，英国法上甚至将知情同意称为“真正的同意”（true consent）。〔19〕

（三）知情同意的基本内涵：充分告知、表意能力、完全理解和自愿同意

知情同意最初译自医疗领域的“informed consent”，字面意思是基于说明的同意或者被告知基础上的同意。日本学者植木哲将其译为“医生的说明”和“患者的同意”，〔20〕我国台湾地区学者一般将其译为“充分说明与同意”，〔21〕我国大陆地区通常译为“知情同意”。根据布莱克法律词典的解释，informed consent 的含义为：医生在对患者实施医疗行为时，应该就医疗处理方案、医疗风险以及其他可以考虑采取的措施向患者做出详细说明，并在此基础上得到患者的同意。〔22〕形式上，中国法语境下的“知情同意”由 informed 和 consent 两个部分组成，早期的知情同意二要素说即源于此。〔23〕然而，字面上对应着“告知”“说明”的 informed，在实践中能否做到使患者“知情”呢？换言之，医生履行了法定告知义务是否就代表患者充分“知情”了呢？答案是否定的，因为“情”的传达需要经过一个主观加工的过程，是否“知”以及“知”多少取决于主观加工是否契合所告知的“情”，“告”只是提供了基础和前提。〔24〕为了准确理解知情同意的基本内涵，需要对《纽伦堡法典》提出的自愿同意四要素作进一步考察。在四要素中，“自愿”是对患者意志自由的保护，任何强迫、胁迫、欺骗等非自愿状态下的同意都是无效的。“法律上有行为能力”为患者行为资格的表征，是对患者决定能力的客观要求。这一概念借鉴了民法上民事行为能力说的分类，即具备完全行为能力人的同意有效，无民事行为能力或者限制行为能力人的同意无效。然而，晚近研究表明，法律上的行为能力并非知情同意能力判定的绝对标准。发达国家的通说认为，医疗上同意能力的确定不是以民事能力为标准，而是以有无理解、认知医疗内容、意义和后果的能力为标准。〔25〕尽管现有研究成果对这一能力的表述并不一致，评价标准也不尽相同，但将其作为知情同意的构成要素并无分歧。〔26〕“理解”要求患者对医生告知的病情、诊治方案、

〔17〕 参见朱伟：《知情同意：困难和出路》，载《哲学动态》2008 年第 2 期。

〔18〕 参见邱仁宗、卓小勤、冯建妹：《病人的权利》，北京医科大学、中国协和医科大学联合出版社 1996 年版，第 53 页。

〔19〕 参见曾凡昌：《医疗过失责任中的知情同意原则研究》，载《河南省政法管理干部学院学报》2011 年第 2 期。

〔20〕 参见〔日〕植木哲：《医疗法律学》，冷罗生等译，法律出版社 2006 年版，第 127 页。

〔21〕 参见陈燕红：《困境与出路：我国患者知情同意权法律保护与使用的完善建议》，载《河北法学》2014 年第 2 期。

〔22〕 See *Black's Law Dictionary*, West Publishing Co., 1989, p. 701.

〔23〕 二要素说以医生为视角，认为知情同意由提供信息和征得同意两个要素构成。参见〔美〕T. A. 波库连科：《知情同意原则对家长作风的挑战》，载《国外社会科学》1994 年第 11 期。

〔24〕 参见胡国梁：《患者知情同意权制度构造之反思——从榆林待产孕妇跳楼案切入》，载《法学杂志》2018 年第 11 期。

〔25〕 参见叶欣：《患者知情同意权的价值目标与法理思辨》，载《学习与实践》2019 年第 4 期。

〔26〕 表征患者此种能力的概念有“识别能力”“同意能力”“表意能力”等。参见赵西巨：《知情同意：要素构成与过程优化》，载《中国医学伦理学》2005 年第 3 期；前引〔25〕，叶欣文。

风险、诊疗所预期达成之后果、疗养中的注意事项等所有与病情有关的信息充分了解、领会。〔27〕关于“知情”，《纽伦堡法典》第1条设定了如下标准和要求：“（使受试者）对于试验的项目有充分的知识和理解，足以作出合理、明智决定之前，必须让他知道试验的性质、期限和目的；试验方法和采取的手段；可以预料的不便和危险，对其健康或可能参与试验人的影响。”〔28〕在自愿同意四要素基础上，后来研究者将告知（或称信息披露）纳入知情同意的构成要素，提出知情同意四要素说和五要素说。〔29〕在行为逻辑上，知情同意可表述为：具有同意能力的患者在对医生告知的信息充分理解和知情的基础上，自愿就是否同意医生告知、请求事项做出选择决定。

在个人信息保护领域，欧盟《95指令》、GDPR和我国的《个人信息保护法》仅在“同意”的定义中规定“知情”作为其基础要素，但对知情同意的内涵并未明确。可资参考的是欧盟数据保护第二十九条工作组第15/2011号意见书。该意见书强调，“自由作出的同意意味着某个具有正常能力的人在不受任何胁迫（无论是社会的、经济的、心理的或其他种类的）情况下所做的自愿决定”。同时，“信息主体作出的同意必须基于一项行动及有关事实及其对含义的理解和认识。信息处理者必须向当事人提供全部事项的、清晰、易懂、准确且全面的信息，尤其是《95指令》第10条和第11条所规定的信息，例如数据处理的性质、目的、可能的数据接收者以及信息主体的权利，包括对有关数据处理作出拒绝可能导致后果的了解”。综上，意见书确定自愿同意的四个必要条件为：充分告知、表意能力、完全理解和自愿决定。这里的“充分告知”要求信息处理者以清晰、易懂、准确、全面的方式向信息主体提供《95指令》第10条、第11条规定的全部信息。同时提出了判断告知是否适当的两项标准：（1）资讯的质素——提供资讯的方式（文字通俗、不使用术语、易懂且清晰）对判断信息主体是否“知情”是至关重要的指标；（2）资讯的可见性和可用性——资讯必须向当事人直接提供，且必须清晰可见、明显且全面。〔30〕“表意能力”强调做出有效同意的主体需具备表示同意的能力。尽管《95指令》并未对无完全法律行为能力人（包括儿童）的同意作出具体规定，但欧盟数据保护第二十九条工作组认为有必要在法律层面进行一般规定，以增强法律的确定性。“完全理解”要求信息主体对告知事项和告知内容充分理解并知情。欲满足此要求，告知形式应简洁、易理解，同时信息主体应具备一定的与告知事项相关的知识储备和理解能力。“自愿决定”指信息主体做出同意决定时必须处于一种完全自由的状态，不能受到任何不正当限制，包括强制、胁迫、欺骗、诱惑等，同意是信息主体完全自愿、发自内心的意思表示。从四个必要条件的特点看，充分告知、表意能力、完全理解属于知情范畴，充分告知是知情的基础和前置要件，知情是信息主体对告知内容理解、认识后的内化过程，要求信息主体必须具有相应的理解能力和表意能力。自愿同意属于同意范畴，自愿为有效同意的先决条件和状态条件，同意则是信息主体在知情前提下自愿作出的肯定性决定，是对信息处理者收

〔27〕 参见前引〔21〕，陈燕红文。

〔28〕 丁镜：《论患者知情同意权的限度》，载《广西社会科学》2012年第4期，第82页。

〔29〕 四要素说认为知情同意包括充分告知、完全理解、表意能力和自愿决定；五要素说认为，知情同意具备信息披露、表意能力、充分理解、自愿和同意决定五个要素。参见前引〔26〕，赵西巨文。

〔30〕 参见《欧盟第二十九条数据保护工作组第15/2011号意见书：“同意”的定义》，澳门特别行政区政府个人数据保护办公室译，载 https://www.gpdp.gov.mo/index.php?a=show&c=index&catid=112&id=12&m=content，最后访问时间：2021年11月28日。

集、利用个人信息的明确授权。因此，本文认为个人信息知情同意应由充分告知、表意能力、完全理解和自愿同意四个要素组成，此四要素共同构成个人信息知情同意的基本内涵。知情同意以信息处理者告知为基础，信息主体充分知情后，继而自由作出有效的同意决定，其基本逻辑为：信息处理者的事先告知—信息主体的知情—信息主体做出同意的意思表示。〔31〕

需要指出的是，由于我们将 informed 译为“知情”，而英文中 inform、notice 均有告知、通知、信息披露等含义，故有观点认为“告知”即为“知情”，其实这是一种误解。从行为学视角看，告知的行为主体是信息处理者，而知情的行为主体是信息主体。告知是信息处理者为信息主体知情同意所提供的信息条件，属于一种信息提供机制；知情则是信息主体对告知内容进行阅读、理解、内化的结果。从告知到知情需要在两个不同主体之间进行角色转换和行为转换，要真正做到充分知情，信息主体必须发挥主观能动性，增强权利意识，提高知情能力。

（四）知情同意的价值目标：保护信息主体权益

知情同意的价值目标是增强个人信息的自主控制，保护信息主体的人格利益和财产利益。其保护重点随社会发展阶段的不同而有所侧重。在小数据时代，个人信息的收集、利用仅局限于政府部门或者具有公共服务职能的社会机构，目的是为公共管理和公共服务等公共职能的履行提供依据。在此种情形下，知情同意的价值更多体现为对个人信息的个人性和人格性的保护，个人隐私保护成为此阶段知情同意的主要价值。由于政府部门对个人信息的收集、利用具有强制性，信息主体的决策空间并不大，其价值更多体现在对个人信息收集、利用行为的知情上，通过信息处理者告知义务的履行以及访问权、更正权等权利的行使，增强个人信息的自主控制能力。进入大数据时代，随着个人信息社会性和资源性的逐步凸显，个人信息的收集、使用行为不再局限于政府部门，数据企业等私营部门成为个人信息收集、利用的重要主体。私营部门对个人信息的收集、利用更多体现在对经济利益的追求上，因此大数据时代信息主体除关注个人信息安全外，也对个人信息的经济价值和出让个人信息为自身带来的利益和风险更加重视。这一阶段知情同意的价值不仅体现为对信息主体隐私利益的保护，更重要的是成为信息主体与信息处理者谈判、争取个人信息经济利益的工具。因此，罗伯特·H. 斯隆（Robert H. Sloan）和理查德·瓦格纳（Richard Warner）认为，如果信息主体有足够的实践经验和知识能对信息披露带来的收益和风险进行恰当平衡，就可认为其同意是知情的。〔32〕

三、知情同意的现实困境与学理反思

个人信息领域的知情同意肇生于小数据时代单一来源的个人信息收集场景，随着大数据时代个人信息来源的多元化、二次利用的广泛化，知情同意面临诸多困境。

其一，作为主要告知载体的个人信息保护政策位置隐蔽查找困难、术语过多晦涩难懂、信息超载文本冗长，告知效果难言乐观。首先，作为主要告知形式的个人信息保护政策或隐私政策

〔31〕 参见高志明、张亚明：《论个人信息法的基本原则》，载《华东理工大学学报（社会科学版）》2013 年第 5 期。

〔32〕 See Robert H. Sloan, Richard Warner, Beyond Notice and Choice: Privacy, Norms, and Consent, 14 (2) *J. High Tech. L.*, 379 (2014).

（以下简称“隐私政策”）多以二次链接或者多次跳转链接的形式呈现，文本隐蔽、获取性差成为网站、手机 APP 的突出问题。〔33〕从点击次数看，用户平均需要点击 3 次才能找到相关的隐私政策。超过三分之一的 APP 需要点击 3 次或者 4 次才能到达隐私政策文本（占比分别为 35.7％和 33.9％），3.6％的 APP 需要点击 5 次。甚至有些 APP 必须在用户注册成为会员后，才可以查看隐私政策。〔34〕其次，隐私政策篇幅冗长、描述复杂、专业术语过多，一般信息主体阅读存在实质困难。即使信息处理者清楚、详尽地告知个人信息处理的方式、范围和后果，信息主体也难以真正理解其中的内容，即使理解了字面含义，也难以准确理解深层内涵和可能给自身带来的影响。〔35〕如美国隐私政策的阅读水平一般设定为 10 级（大学阅读水平），但社会平均阅读水平介于 8～9 级之间，〔36〕二者之间的差距限制了许多人对政策的阅读和理解。〔37〕我国隐私政策的可读性也不容乐观，一项对 63 款手机 APP 隐私政策的定量研究显示，多数隐私政策阅读水平要求为大学一年级水平，对现阶段国内大多数网民而言，隐私政策的可读性低、阅读理解难度大。〔38〕我国目前未设定隐私政策阅读标准，但有研究指出，“对于信息主体而言，信息收集者的告知若不能使具有一般知识水平和生活经验的信息主体掌握或基本掌握其信息被收集、利用的情况，即可判定信息收集者未良好履行告知义务”〔39〕。

其二，信息主体知识匮乏，对告知内容难以理解，主动知情意愿低。大数据时代，各种移动应用覆盖了人们生活的方方面面。为了自由、知情地决定是否同意各种应用对个人信息的收集，信息主体需要具备多种知识和能力，以对信息收集带来的收益和潜在危害进行准确评估。然而，多数信息主体缺乏相应的知识和能力，知识的缺乏导致许多人难以理解或应对信息披露。〔40〕大数据时代是知识和信息的爆炸时代，各类特色平台和 APP 层出不穷，需要信息主体不断拓展知识空间，“就收集主体个人信息本身而言并无特别令人费解的专业知识，因此其侧重点应当是令公众知晓其行为，而非理解”的观点属于误解。〔41〕尤其是多数隐私政策中都有履行法定义务需要收集的个人信息规定，比如《花椒直播用户隐私协议》载明，根据中华人民共和国相关的法律法规，在使用直播功能或服务时，需要收集真实身份信息（真实姓名、身份证号）、面部信息（用于芝麻信息识别）以完成实名验证。〔42〕这需要信息主体了解隐私政策依据的法律名称和具体规定，

〔33〕 参见刘娇、白净：《中外移动 APP 用户隐私保护文本比较研究》，载《汕头大学学报（哲学社会科学版）》2017 年第 3 期。

〔34〕 参见朱颖：《我国移动 APP 隐私保护政策研究——基于 96 个移动应用 APP 的分析》，载《暨南学报（哲学社会科学版）》2017 年第 12 期。

〔35〕 参见武腾：《最小必要原则在平台处理个人信息实践中的适用》，载《法学研究》2021 年第 6 期。

〔36〕 See M. Ryan Calo, Against Notice Skeptcism in Privacy (and Elsewhere), 87 *Notre Dame Law Review*, 1053 (2012).

〔37〕 也有研究者认为美国常用网站的隐私政策声明（the privacy policy statement）需要 11～12 级教育水平才能准确阅读和理解。See Stephen A. Rains, Leslie A. Bosch, Privacy and Health in the Information Age: A Content Analysis of Health Web Site Privacy Policy Statements, 24 *Health Communication*, 436 (2009).

〔38〕 参见秦克飞：《手机 APP 隐私政策的可读性研究》，载《情报探索》2019 年第 1 期。

〔39〕 江帆、常宇豪：《个人信息保护中“知情同意”适用的困境与出路》，载岳彩申、盛学军主编：《经济法论坛》第 21 卷，法律出版社 2018 年版，第 60 页。

〔40〕 参见〔美〕欧姆瑞·本·沙哈尔、卡尔·E·施奈德：《过犹不及——强制披露的失败》，陈晓芳译，法律出版社 2015 年版，第 95 页。

〔41〕 参见万方：《隐私政策中的告知同意原则及其异化》，载《法律科学（西北政法大学学报）》2019 年第 2 期。

〔42〕 参见《花椒直播用户隐私协议》，载 http://www.huajiao.com/agree/privacy，最后访问时间：2022 年 2 月 22 日。

以判断其要求是否合法，是否存在假借法律名义过度收集个人信息和信息滥用问题。

其三，平台和 APP 强制“二选一”削弱了知情同意功能，同意成为使用产品或者服务的符号，而非自己意思的真实表示。在许多平台和 APP 应用中，要求信息主体在“同意”和“不同意”之间进行选择，即“二选一”现象。同意代表对隐私政策的认可和收集相关个人信息的授权，是使用其产品或服务的前提；不同意则为相反意思之表示，相应地，无法使用其产品或享受其服务。目前平台隐私政策多为制式形式，信息主体对其内容无建议权和修改权，若同意，则表示全部接受其内容，无论是否合理；若不同意，则无法使用其产品或享受其服务。消费者若想使用其产品、享受其服务，只能点“同意”，别无选择。因此，在该种语境下隐私政策是否合理以及是否阅读、能否理解，对信息主体来讲已无关紧要，因为自己根本无法改变。按照知情同意机制设计的初衷，同意应是在无外力控制下自由地做出，但受互联网经济网络效应、消费者锁定效应影响，许多具有垄断地位企业的产品或服务，直接关系到消费者根本利益，加之转移成本高昂，拒绝这些服务变得越来越难。在这种情形下，这些根本利益本身的重要性以及其他消极压力和影响构成外力控制，胁迫信息主体在“同意”与“不同意”中做出选择。〔43〕只能选择“同意”的前提下，隐私政策的阅读和知情变得毫无必要，同意成为使用产品或享受服务的代名词。

其四，信息来源多元化、处理流程复杂化以及广泛的个人信息二次利用架空了知情同意。在大数据时代，信息收集、使用方式趋向多元化，除传统的“一对一”收集外，数据共享、cookies 抓取、刷脸支付（门禁等）、监控设备、无人机或无人驾驶汽车等新型收集方式成为个人信息收集的重要途径，且占据了信息收集的主导地位。美国亚利桑那大学的一项研究表明，健康类网站的消费者个人信息中有 80％来自自动抓取（collect automatically）。上述新型数据收集方式很难告知并征得信息主体同意。大数据聚合、挖掘所进行的“数据二次处理”也是如此。〔44〕

其五，不加区分的适用知情同意使信息主体陷入告知同意疲劳。根据法律规定，知情同意是个人信息收集、使用最主要的合法途径，多数信息收集、使用行为需要告知信息主体并获得同意，频繁告知、多次索取同意导致出现告知同意疲劳。据工业和信息化部统计，截止到 2021 年 12 月底，我国市场上监测到的移动应用 252 万款，其中本土第三方应用商店移动应用数量超过 117 万款，苹果商店（中国区）移动应用数量超过 135 万款，范围覆盖了人们日常生活涉及的诸多领域。〔45〕消费者初次使用任何一款 APP 均需在阅读其隐私政策后提供必需的个人信息；还有一些隐私政策根据法律规定属于定向推送或者邮寄送达，比如根据美国《金融服务现代化法案》规定，金融机构在向第三方分享消费者非公开个人信息前，必须明确告知消费者且之后不论隐私政策内容是否发生变化，需要每年至少邮寄送达一次。〔46〕频繁告知、多次同意给消费者带

〔43〕 参见王籍慧：《个人信息处理中同意原则的正当性——基于同意原则双重困境的视角》，载《江西社会科学》2018 年第 6 期。

〔44〕 参见常宇豪：《论信息主体同意权的绝对化困境与相对性重构——兼论〈个人信息保护法（二审稿）〉同意制度的完善》，载《江西财经大学学报》2021 年第 5 期。

〔45〕 参见工信部：《2021 年我国 APP 总量持续下降 其中游戏类 APP 数量仍居首位》，载 https://www.sohu.com/a/520633632_121291394，最后访问时间：2022 年 2 月 17 日。

〔46〕 See Gramm-Leach-Bliley Act of 1999 (Financial service Modernization Act of 1999), Pub. L. No. 106 - 102, 113 Stat. 1338 (codified as amended in scattered sections of 12, 15 U. S. C.).

来沉重负担。据美国 2008 年进行的一次调查，消费者全部阅读常用网站隐私政策需要花费 244 个小时，甚至每年超过 30 个工作日。美国联邦贸易委员会主席乔恩·莱博维茨（Jon Leibowitz）在 2009 年指出：我们都知道，消费者根本不去阅读隐私政策。〔47〕

面对知情同意在实践中的诸多困境，国内外学界进行了集体性反思与争论。主张废除知情同意规则的学者认为该规则在大数据时代既无法有效保护个人信息，又阻碍了数据流通及创新应用，不应再成为个人信息处理的合法性基础。〔48〕支持者出于知情同意在个人信息保护法律体系中的重要性、维护人格完整性和人的主体性，以及平衡信息主体与信息处理者权利势差之需要，认为知情同意不应轻言放弃，但需要进行改良和完善，并提出若干改良方案。〔49〕较为典型的是基于场景风险理论的差别性适用探索，如有学者提出可根据不同场景中个人信息处理风险的高低适用不同的同意要求；〔50〕也有学者建议采用“场景合理＋拟制同意＝合法利用”模式化解知情同意的僵硬适用问题〔51〕。另一较为常见的探索是动态同意模式的适用，主张在信息主体和信息处理者之间搭建一个交流平台，信息主体可视个人信息处理情况随时选择加入或者退出。〔52〕还有学者提出通过经济激励方式完善知情同意规则的建议。〔53〕笔者认为，大数据时代知情同意的功能下降是不争的事实，但鉴于知情同意在个人信息保护法律体系中的基础性地位，放弃则意味着整个法律体系根基之动摇，况且“以用户的知情、同意、选择、控制为核心来建构整体个人信息保护制度，以对抗强大的商业组织和政治力量的模式，其必要性取得了大多数人的共识，且在可见的未来，其他情形都难以撼动同意原则的主流和基础地位”〔54〕。尤其在我国法已将知情同意确立为个人信息保护的核心规则背景下，理性的做法是立足于解释论原理研究提出消解或缓解知情同意困境的对策措施，赋予知情同意新的生命力。在方法论上，场景风险理论之运用、动态同意理论的探索以及经济激励方式均对解决知情同意困境有着积极意义，但并不符合我国严格个人信息保护的立法方向，在现有制度框架内通过规则解释和制度续造等方式探究知情同意的实现路径是较为妥帖之策。这也是本文以解释论视角探究知情同意实现路径的初衷。

四、知情同意实现的多元共治路径

知情同意的实现涉及主体较多，本文将按照信息处理者、信息主体、公共机构和社会组织四类主体探究实现路径。

〔47〕 See Fred H. Cate, The Limits of Notice and Choice, *IEEE Security & Privacy Magazine*, 59－62 (2010).

〔48〕 持此观点的如范为：《大数据时代个人信息保护的路径重构》，载《环球法律评论》2016 第 5 期；田野：《大数据时代知情同意原则的困境与出路——以生物资料库的个人信息保护为例》，载《法制与社会发展》2018 年第 6 期；任龙龙：《论同意不是个人信息处理的正当性基础》，载《政治与法律》2016 年第 1 期。

〔49〕 参见前引〔11〕，徐丽枝文；王成：《个人信息民法保护模式选择》，载《中国社会科学》2019 年第 6 期；吕炳斌：《个人信息保护的“同意”困境及其出路》，载《法商研究》2021 年第 2 期。

〔50〕 参见前引〔48〕，范为文。

〔51〕 参见蔡星月：《数据主体的“弱同意”及其规范结构》，载《比较法研究》2019 年第 4 期。

〔52〕 参见前引〔48〕，田野文。

〔53〕 参见蔡培如、王锡锌：《论个人信息保护中的人格保护与经济激励机制》，载《比较法研究》2020 年第 1 期。

〔54〕 申卫星：《大数据时代个人信息保护的中国路径》，载《探索与争鸣》2020 年第 11 期，第 6－7 页。

（一）信息处理者依法履行告知义务

在现行法律制度框架内，信息处理者告知义务的履行是知情同意实现的主要路径。在《个人信息保护法》中，信息处理者的告知义务主要包括第 17 条规定的个人信息处理前的一般告知义务，第 22 条规定的因合并、分立、解散、被宣告破产等原因需要转移个人信息前的告知义务，第 23 条规定的个人信息处理者向第三方提供其处理的个人信息前的告知义务，第 30 条规定的处理个人敏感信息前的告知义务等。这些告知义务中的内容和形式要求成为信息处理者履行告知义务的基本法律遵循。

一方面，信息处理者应严格遵守法律规定的告知事项，确保内容真实、准确、完整，不得遗漏、伪造相关信息，也不得采用陈旧过时的信息误导信息主体。一般告知内容应包括个人信息处理者的名称或者姓名和联系方式，个人信息的处理目的、处理方式，处理的个人信息种类、保存期限，个人行使法律规定权利的方式和程序等。对于特殊情形下的告知事项，法律作了特别规定，如：涉及转移个人信息的，除一般告知事项外还应当向个人告知接收方的名称或者姓名和联系方式；需要向其他处理者提供个人信息的，需增加告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意；需要处理敏感个人信息的，还需告知处理敏感个人信息的必要性以及对个人权益的影响等事项。

另一方面要严格依照法律规定的形式进行告知。《个人信息保护法》第 17 条规定“应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知”，此规定为解决告知文本不友好痼疾提供了指引。首先，告知文本位置应显著，便于查找和阅读。信息处理者应严格按照《信息安全技术 个人信息安全规范》（GB/T35273—2020）的要求，将隐私政策链接在网站主页、移动应用程序安装页、社交媒体首页等显著位置进行设置。〔55〕 其次，告知语言应清晰易懂，提高阅读体验感。做到条理清晰、语言简洁、通俗易懂、要求明确，而且告知请求事项要单独列出，不与其他事项混杂，使阅读者一目了然。近年来，针对隐私政策隐晦、难懂、可读性差等问题，学界和业界进行了多种创新，如通过法律术语通俗化、〔56〕 分层通知、〔57〕 表格化、图示化、标签化〔58〕和其他标准化披露、缩短篇幅等形式，〔59〕 使隐私政策更易懂，内容更直观、突出。笔者进行的一项调查表明，有 85.47％的被调查者认为将在隐私政策编写简洁、保证可读懂且不会占用过多时间的前提下认真阅读隐私政策。可见，改善告知语言和形式有利于消解隐私文本阅读体验差之顽疾。再次，告知形式应进行创新，满足不同群体诉求。隐私政策是针

〔55〕 参见《信息安全技术 个人信息安全规范》（GB/T35273—2020）第 5.5（d）条。

〔56〕 See Mike Yang, Trmming Our Privacy Plolicies, Offcial Google Blog, Sept. 3, 2010, available at http//googleblog. blogstop. com/2010/09/trimming-privacy-policies. html, last visited on Nov. 8, 2021.

〔57〕 See Center for Information Policy Leadership, Hunton & Williams LLP, Ten Steps to Develop a Multilayered Privacy Notice 1, 2007, available at http://www. informationpolicycentre. com/files/Uploads/Documents/Centre/Ten Stepsw hitepaper. pdf, last visited on Dec. 5, 2021.

〔58〕 See Patrick Gage Kelley et al., Carnegie Mellon Univ, Standardizing Privacy Notice (2010), available at http://repository. cmu. edu/cgi/viewcontent. cgi? articlr = 1002&conntext = cylab, last visited on Nov. 20, 2021; Alan Levy, Manoj Hastak., Consumer Comprehension of Financial Privacy Notices (2008).

〔59〕 See Corey A. Ciocchetti, The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practies, 26 *J. Marshail J. Computer & Info. L.*, 45 (2008).

对不特定主体进行告知的，由于不同人群需求不同、知识结构各异，对隐私政策的详略程度、专业化水平以及个人信息处理可能引发的风险要求并不完全一致。比如，执法人员、司法人员、研究人员、信息专业人士和第三方评估机构要求告知内容详尽、描述准确、用语专业；而一般信息主体则希望隐私政策内容简短、重点突出、语言平实、易于理解。多元化需求的存在，导致同一隐私政策难以协调明确性与具体性、简洁性与全面性、通俗性与专业性之间的冲突。为了回应不同群体之诉求，信息处理者需要进行告知形式创新。一个可行的方案是采用“长短版结合”的形式进行告知。长版隐私政策属专业型隐私政策，供执法者、司法者和专业人士阅读，突出内容的全面性、完整性、专业性，可以链接形式呈现；短板隐私政策属公众型隐私政策，主要服务于一般信息主体，需凸显内容的简洁性、明确性和通俗性，可在突出位置设置，便于公众阅读。对于特殊情形下对特定主体的告知，则采用因人而异的个性化告知形式，以精确匹配异质需求。〔60〕同时，隐私政策应目的明确、请求事项具体，以确保信息主体同意的真实、有效。

（二）信息主体增强知情能力和行权意识

《个人信息保护法》第44条赋予了个人对其个人信息处理的知情权和决定权，个人有权限制或者拒绝他人对其个人信息的处理。因此，信息主体可在信息处理者依法告知的基础上依决定事项之需要，向信息处理者索取与自己有关的处理信息，以在充分知情的前提下做出是否同意信息处理者处理自己个人信息的理性选择。这要求信息主体具备足够的知识储备和知情能力，同时增强知情权和决定权的行权意识。

1. 增强知识储备和知情能力

知情是信息主体在信息处理者充分告知的基础上充分内化的结果。如何在告知基础上做到充分知情，信息主体有效增强知识储备、提高自身知情能力是关键。隐私政策内容一般包括拟收集信息的类型及数量、用途、收集者或与之共享的第三方信息等，要做到读懂、理解至少需要常识性和专业性两方面知识。其一，对于平台或者APP的通用功能，一般需要收集姓名、手机号码、出生日期等身份信息；当使用支付功能时，需收集姓名、银行卡类型及卡号、有效期及银行预留手机号码等信息；当需要发布音视频、图片文字和进行直播时，则需要授权使用相机、麦克风权限和设备所在位置信息权限。这些常识性知识是生活在大数据时代公民的必备知识。其二，根据功能差异，不同平台对独具特色的功能有特殊规定，如《微信隐私保护指引》第1.2条规定，当使用微信服务时，需要收集设备型号、操作系统、唯一设备标识符、登录IP地址、微信软件版本号、介入网络的方式和类型、设备加速器、操作日志等信息。〔61〕《蚂蚁金服隐私权政策》规定，为了进行业务风险评估，需要记录使用设备型号、IP地址、设备软件版本信息、设备识别码、设备标识符、位置、网络使用习惯以及其他与服务相关的日志信息等。要理解上述规定，首先需要了解相关功能的基本内容，其次需要知晓使用这些功能需要的基

〔60〕 See Christoph Busch, Implementing Personalized Law: Personalized Disclosures in Consumer Law and Privacy Law, 86 (2) *The University of Chicago Law Review*, 551-580 (2019).

〔61〕 参见《微信隐私保护指引》，载 https://weixin.qq.com/agreement?lang=zh_CN&cc=CN&s=privacy&v=1&need，最后访问时间：2022年1月28日。

本信息类型。这样才能准确甄别政策文本中规定收集的个人信息种类是否必要、是否存在过度收集情形。

2. 提高知情权和同意权行权意识

目前对隐私政策的法律性质尚存在争议，从国外法律实践看，美国普遍将隐私政策视为合同，正如马克·莱姆利（Mark Lemley）指出的："双方同意合同条款是合同法的基本原则，同意赋予了合同私法上的合法性。"〔62〕这意味着只要信息主体有同意行为，即可认定其认同了隐私政策之约定，自然需要受该合同之约束。因此，信息主体应主动阅读、理解隐私政策的内容，了解其中规定的个人信息收集、使用、共享政策，收集的具体信息种类，以及个人信息处理可能带来的风险，在充分知情后慎重做出选择，避免因未认真阅读隐私政策而盲目同意带来不利后果。对于隐私政策中难以理解的专业术语，应积极行使知情权，要求信息处理者以通俗语言进行解释；对于法定告知内容无法满足同意权行使需要的情形，应及时向信息处理者要求所需信息，真正将个人同意建立在充分知情基础上，使同意充分体现自己的自由意志。

（三）公权力机构完善法律制度，严格执法司法

"建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为"是《个人信息保护法》赋予公共机构的职责，公共机构应通过完善法律制度、加强行政执法、强化司法保护等方式，保证信息主体知情同意之实现。

1. 完善法律制度，弥合告知事项与民众关切之错位

我国《个人信息保护法》规定的个人信息处理前告知事项包括：信息处理者名称或者姓名和联系方式；个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；信息主体权利的行使方式和程序等。但根据国内外对公众隐私关注的研究，信息主体在做出同意决定之前更多关注的是隐私保护和隐私损失（privacy loss）等问题。根据巴特·卡斯特斯（Bart Custers）、西蒙娜·范德霍夫（Simone Van der Hof）和巴特·舍默（Bart Schermer）等人的调查，向网站提供个人信息可能造成的隐私损失和个人隐私保护两个问题的关注值在里克特七分量表上分别达到 5.78 和 5.28，表明信息主体对此两类问题高度关注。〔63〕塔玛拉·迪内夫（Dinev）和保罗·哈特（Hart）的研究也表明消费者关注重点是非授权访问、黑客攻击、安全漏洞、非授权二次使用、信息错误等与隐私泄露、隐私危害等与隐私安全相关的问题。〔64〕然而，现行《个人信息保护法》并未将个人信息安全保护措施、信息泄露可能给信息主体造成的危害等公众关心的问题纳入告知范围，法定告知内容与信息主体的隐私关注存在错位，现有告知信息无法满足信息主体同意决策之需要。应以《个人信息保护法》第 17 条第 1 款第（4）项"法律、行政法规规定应当告知的其他事项"为依托，在未来出台配套行政法规时，将个人信息处理可能给信息主体带来的风险以及与之相关的安全隐患列入依法必须告知范围，以回应信息主体之关切。

〔62〕 Mark A. Lemley, Terms of Use, 91 *Minn. L. Rev.*, 459, 464－465 (2006).

〔63〕 See Bart Custers, Simone Van der Hof, Bart Schermer, Sandra Appleby-Arnoid, Noelie Brockdorff, Informed Consent in Social Media Use-The Gap between User Expectations and EU Personal Data Protection Law, 10 (4) *SCRIPT-ed*, 441 (2013).

〔64〕 See Dinev T, Hart P, Internet Privacy Concerns and their Antecedents-measurement Validity and a Regression Model, 23 (6) *Behaviour & Information Technology*, 413 (2004).

2. 加强行政执法，削减权利势差

进入大数据时代，信息主体与信息处理者之间在信息拥有、技术能力等方面差距拉大，已然形成巨大的权利势差。在强势的信息处理者面前，强制“二选一”、超范围收集个人信息、不告知收集处理个人信息等问题突出，知情同意被架空，市场失灵现象明显。政府作为市场秩序的维护者和规则的制定者，有必要对个人信息处理者的义务履行进行监管，以解决告知义务履行不充分、模糊告知、强制同意等削弱知情同意的问题，迅速恢复个人信息利用秩序。一方面，严格执行《App 违法违规收集使用个人信息行为认定方法》《App 违法违规收集使用个人信息自评估指南》等政策规范，继续对违规收集用户个人信息、违规使用用户个人信息、不合理索取用户权限等突出问题进行整治，公开曝光、约谈、下架、关闭一批问题严重且整改不彻底的 App 和网站，使无隐私政策、捆绑授权和强制索权、超范围收集使用个人信息等典型问题得到根本改善。另一方面，坚持问题导向，对人脸识别等生物特征信息收集使用不规范，深度伪造，App 后台自启动、关联启动、私自调用权限上传个人信息，录音、拍照等敏感权限滥用等社会反映强烈的重点问题进行集中整治，通过行政权力制约数据权力的方式，防止信息处理者利用权利势差刻意规避知情同意现象的发生。

3. 转化保护模式，强化司法保护

目前，我国司法审判普遍采用义务模式保护信息主体的知情同意。在义务模式下，法院将信息处理者法定义务之履行作为判断信息主体是否知情的标准。只要信息处理者履行了法定告知义务，且信息主体有机会阅读并了解告知内容，不论个人是否真正阅读或是否读懂、理解，法院都将认定信息主体做出的同意为“知情同意”。在“朱某与北京百度网讯科技有限公司隐私权纠纷案”中，二审法院即认为：“百度网讯公司在《使用百度前必读》中已经明确告知网络用户可以使用包括禁用 cookie、清除 cookie 或者提供禁用按钮等方式阻止个性化推荐内容的展现，尊重了用户选择权。朱某在百度网讯公司已经明确告知上述事项后，仍然使用百度搜索引擎服务，应视为对百度网讯公司采用默认‘选择同意’方式的认可。”〔65〕此种裁判思路即为义务保护模式。但在一审法院采用的权利保护模式下，尽管百度网讯公司网页中的《使用百度前必读》有说明和提醒的内容，但文字放在了网页的最下方，不仅字体明显较小，而且还夹在“◎2014baidu”与“京 ICP 证 030173 号”中间，难以识别并加以注意，无法起到规范的说明和提醒作用，不足以让消费者明了存在“选择同意”的权利，因此认定被告侵犯了消费者知情权和选择权。同一个案件，一审法院和二审法院得出了完全相反的结论，原因即在于两个法院采用了不同的裁判思路。当二审法院采用义务保护模式时，明知消费者的知情利益未受到应有的保护，但由于经营者未违反法定告知义务，仍然不能为消费者的知情利益提供充分的保护。〔66〕因此，在司法维度上，只有以信息主体为中心，变义务保护模式为权利保护模式，方可实现对信息主体知情同意的充分保护。尤其在《个人信息保护法》已经正式赋予信息主体知情权和决定权的背景下，权利保护模式更具有必要性和现实性。

〔65〕 江苏省南京市中级人民法院（2014）宁民终字第 5028 号民事判决书。

〔66〕 参见李友根：《论经济法权利的生成——以知情权为例》，载《法制与社会发展》2008 年第 6 期。

（四）社会组织强化行业自律和第三方认证

1. 制定科学的行业告知文本

遵守知情同意规则、强化个人信息保护符合企业和行业的根本利益。良好的行业自律既可以为立法提供指引，避免盲目立法抑制信息产业发展，又可以以之提升经营者商誉，吸引消费者“用脚投票”。〔67〕因此，应当鼓励企业适应大数据时代的特点，确立数据安全观念，把数据当作核心资产，秉持用户个人信息至上的基本价值观，培育保护个人信息就是维护核心竞争力的意识，积极主动承担个人信息保护责任。〔68〕

一个可能的方向是由行业协会针对不同类型信息处理者开展不同业务时的不同需求，编写本行业自律公约和隐私政策示范文本。例如《国民经济行业分类》（GB/4754—2011）中邮政业的快递服务需要收集信息主体的姓名、地址、电话号码，而不需要收集网络邮箱号或指纹信息；又如淘宝、京东等互联网销售平台与优步、滴滴出行等互联网约车平台虽然同属于互联网生活服务平台，但业务模式、交易方式、实现功能都完全不同，即可在统一的保护细则或自律公约下分别编写不同的示范文本。信息处理者按照行业惯例收集本行业一般经营者所需的个人信息时可按照上述个人信息分类标准进行监管，而收集额外信息或将信息用于非常规用途时则必须向信息主体详细告知并征得同意，所受监管也将更加严格。这种保护模式一方面细化了个人信息保护场景，实现了法律稳定性、可预测性和针对性保护的有机统一，另一方面在隐私风险无法完全避免的前提下可将风险控制在最低限度。

2. 强化第三方认证

充分发挥第三方认证机构专业性强、技术力量雄厚的优势，构建知情同意第三方认证体系，以此作为个人信息事前保护的重要内容。信息处理者如果希望取得认证机构的认证则需要符合该机构的个人信息保护标准。一旦认证机构形成公信力并为信息主体所熟知，具有该认证机构的认证就会成为信息处理者的核心竞争力，从而激励信息处理者自觉履行告知义务，提高个人信息保护水平。在通过认证的背景下，信息主体虽然可能仍无法完全理解隐私政策的全部内容，但可以通过信息处理者的认证资格对其个人信息保护水平产生信任，并基于信任做出同意。对于认证的作用，索罗夫教授以食品和汽车为例指出，我们并不具备食品和汽车安全的专业知识，但是食品和汽车制造商需要根据安全标准进行生产，消费者只需要了解其是否符合标准即可。〔69〕美国对于隐私认证已经发展出了一套较为完备的体系可供借鉴，我国也已经成立了互联网诚信联盟（iTrust）可提供个人信息安全认证，其核心成员包括了人民网、阿里巴巴、新浪、腾讯、百度、搜狐、网易、凤凰网等国内较有影响力的网络服务提供商，但其影响力（尤其是对信息主体而言）还有待提升。

五、结　语

信息主体的知情同意是我国个人信息保护法的法律基础，也是访问权、撤回权、修改权、携

〔67〕 参见张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，载《中国法学》2015 年第 3 期。

〔68〕 参见周汉华：《探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向》，载《法学研究》2018 年第 2 期。

〔69〕 See Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 *Harvard Law Review*, 1880 (2013).

带权、删除权等个人信息权具体权能存在的前提和条件。〔70〕尽管在大数据时代知情同意陷入困境，但轻言放弃并非明智之举。《个人信息保护法》创设信息主体知情权和决定权，昭示着我国个人信息保护立法坚持自主控制、弘扬“以人为本”理念的强化。当然，由于信息处理者和信息主体之间存在严重的权利势差，加之信息主体专业知识和信息技能的匮乏，仅仅依靠个人无法充分实现知情同意，必须借助公权力介入以监督信息处理者法定告知义务的履行，通过加强行政执法改善制约信息主体知情同意实现的社会环境、制度环境和技术环境，遏制信息处理者利用数据权力刻意规避、架空知情同意现象的发生。同时，积极发挥行业协会和第三方机构专业性强、技术力量雄厚之优势，共同营造有利于知情同意实现的氛围，打造具有中国本土特色的知情同意实现机制。《个人信息保护法》创设知情权和决定权仅是提高知情同意保护水平的开端，未来应通过配套法规、规章建设和法律解释，明确信息主体主动知情的程序和路径，同时将司法保护从义务模式转向权利模式，方能真正实现信息主体的知情同意，助力《个人信息保护法》的实施。需要指出的是，强调信息主体知情同意的实现并非将之绝对化，个人信息的处理应以《个人信息保护法》第13条确立的多元合法性基础为依托，本文意图在于探讨以同意为合法性基础的处理情形中如何使同意建立在知情前提上，保证信息主体的同意决定真正体现自己的自由意志。

Abstract: Informed consent is a basic rule commonly adopted in personal information protection laws of various countries, and it is also the core rule of personal information protection laws in China. The legal basis of informed consent system comes from the guarantee of information subject's autonomy of will, and information subject's independent control of personal information can be realized through effective consent after full notification. In the era of big data, with the diversification of personal information sources and the extensive reuse, informed consent is facing a series of dilemmas, such as obscure privacy policy, lack of knowledge of information subjects, forced “two choices” by information processors, difficulty in applying informed consent to new personal information processing behaviors, and notification fatigue caused by frequent informed consent. Given the important value of informed consent and its cornerstone status in the personal information protection regime, giving up lightly is not a wise move. Multi-governance mode should be adopted to ensure the realization of information subject's informed consent, such as information processors informing according to law, information subjects enhancing their awareness of knowing and exercising, public institutions perfecting legal system and strictly enforcing the law, and social organizations strengthening industry self-discipline and third-party certification.

Key Words: personal information, autonomy of will, informed consent dilemma, multi-governance

（责任编辑：武　腾　赵建蕊）

〔70〕 参见前引〔49〕，王成文。

财经法学 No. 1，2022
pp. 18 - 31

个人信息保护“目的限制原则”的反思与重构
——以《个人信息保护法》第 6 条为中心

朱荣荣*

内容提要： 目的限制原则作为个人信息处理的基本原则，要求信息处理活动不得溢出信息收集时的初始目的，以保障信息主体对个人信息的自主控制与支配。然而，大数据时代个人信息的多维度利用日趋常态化与复杂化，导致信息处理目的难以在信息收集阶段完全确定下来，严格的目的限制原则忽视了个人信息的利用价值。信息保护与信息利用均为法律追求的价值目标，不能顾此失彼，因此，有必要在个人信息类型化视角下重塑目的限制原则的规范内涵。申言之，处理个人敏感信息必须恪守目的限制原则，禁止超越初始目的范围处理之；处理个人一般信息原则上亦须遵从目的限制原则，但特殊情形下允许超越初始目的而处理信息，前提是不得引发高于信息主体所预期的风险。

关键词： 目的限制原则　信息保护　信息利用　个人敏感信息　风险限定

大数据时代，对于个人信息的获取与利用愈益普遍，信息处理者在挖掘、分析个人信息时可能在一定程度上侵害信息主体的合法权益。为规制不当的信息处理行为，《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）第 6 条确立了目的限制原则，该条规定“处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息”。目的限制原则作为个人信息保护制度的基石，〔1〕能够有效避免滥用个人信息现象的发生。

随着大数据分析技术的不断发展，社会对于个人信息的利用需求达到了前所未有的高度，目的限制原则要求处理个人信息应当具有明确、合理的目的，且后续的信息处理应当与初始目

* 朱荣荣，南京大学法学院博士研究生。

〔1〕 Vgl. Peter Schantz, DS-GVO Art. 5 Grundsätze für Die Verarbeitung Personenbezogener Daten, in Heinrich Amadeus Wolff, Stefan Brink (eds), BeckOK Datenschutzrecht (33rd edn, 2020), Rn. 12.

的直接相关，极大地压缩了信息利用的空间，不符合信息保护与信息利用动态平衡之立法理念。有鉴于此，有必要对目的限制原则进行深度考察，寻求其在新时代背景下合理的因应之道。

一、目的限制原则的内涵阐释与法理基础

（一）目的限制原则的基本内涵

根据《个人信息保护法》第6条可知目的限制原则包含两个方面，即目的明确与使用限制。前者指收集个人信息应当具有明确、合理的目的，不得过度收集个人信息；后者指个人信息的处理应当与初始目的直接相关，如果信息处理行为超出了初始目的则为法律所不许。可见，目的明确与使用限制是不可分割的有机整体，两者相辅相成、相互制约，目的明确原则是信息处理行为的逻辑起点，只有在收集阶段明确告知信息处理的具体目的并获取信息主体的有效同意方可处理他人信息。同时，为确保信息处理目的的效力性，后续的信息处理行为应当与处理目的直接相关，不得超越初始目的可能的范围恣意处理个人信息，否则目的明确原则将形同具文。

目的明确原则是维护个人基本尊严的重要工具，在收集和利用个人信息时，忽视或淡化“目的”意味着人格尊严将受到严重的侵蚀。〔2〕信息主体与信息处理者之间信息不对称的客观事实要求信息处理者在收集信息之时应当善尽说明义务，避免信息主体因信息的不充分而做出错误的决策。目前，我国《民法典》第1035条、《网络安全法》第41条、《消费者权益保护法》第29条等诸多规范都要求信息处理者明示信息处理的目的，但对于“目的”的具体要求则未言明。《个人信息保护法》第6条规定，目的明确原则应当满足两个要件，即目的明确与目的合理。目的明确性要求收集个人信息应当具有明确的、特定的目的，过于宽泛与模糊的目的可能被认为是不合法的，目的明确性迫使信息处理者在收集信息之前审慎思考信息处理的目的，可以在一定程度上制约信息处理者恣意处理信息。信息处理者在形成明确的信息处理目的之后，还须将此目的以一种可被理解的方式清楚地表达出来，确保相关主体对信息处理目的的认知不存在歧义。关于目的明确性的形式要求，立法没有明文规定，从规范目的来看，目的明确性旨在保障信息主体充分知悉信息处理的目的，因此，信息处理者借助于何种形式表明其目的在所不问。目的合理性要求信息处理目的必须符合社会一般人的事理认知，不得违反基本的伦理道德与公序良俗。目的合理性包含两个要素，即制度层面的目的合法与价值层面的目的正当。目的合法是信息处理的最低要求，信息处理者处理他人个人信息应当具备合法性事由，包括约定事由与法定事由，约定事由指双方当事人可以自行约定信息处理的具体事项，法律不得无故加以干涉。法定事由则指法律所规定的无需获取信息主体同意即可处理信息的事由，包括订立或履行合同所必需、履行法定职责

〔2〕 See Joseph A. Cannataci, Jeanne Pia Mifsud Bonnici, The End of the Purpose-Specification Principle in Data Protection, 24 *International Review of Law, Computers & Technology*, 102 (2010).

或法定义务等。目的正当性指收集个人信息必须具有充足的价值基础，合理兼顾信息主体与信息处理者的利益，目的正当性的判定依附于个案具体情境，随着社会的发展以及立法理念的变迁而动态调整。

目前，我国对于使用限制的判定标准采取的是“关联性”，要求信息处理行为不得与初始目的不具有关联性。然而，立法对于“关联性”的具体内涵没有予以明确，《个人信息保护法》认为信息处理行为应当与信息收集时的初始目的具有“直接关联性”，张新宝教授起草的《个人信息保护法（专家建议稿）》主张信息处理行为应当与初始目的具有“合理关联性”。《信息安全技术 个人信息安全规范》（2020 年）则认为，“关联性”包括“直接关联性”与“合理关联性”，其规定“使用个人信息时，不应超出与收集个人信息时所声称的目的具有直接或合理关联的范围”。对于何谓“合理关联”，《信息安全技术 个人信息安全规范》（2020）并没有给出明确的答案，而是具体描述了属于“合理关联”的信息利用情形，其认为“将所收集的个人信息用于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述，属于与收集目的具有合理关联的范围之内”。不同于我国，域外立法采取的是“兼容性”标准，第 29 条数据保护工作组指出，不同于初始目的的进一步处理并不意味着与初始目的自动地不兼容，某些情况下，信息处理虽然与初始目的不同，但二者可能是相符的。〔3〕关于“关联性”与“兼容性”的关系，有学者认为，在大数据产业下，数据机构对数据的二次利用往往跟初始目的没有关联性，但这并不意味着一定不相兼容。〔4〕换句话说，较之“关联性”，“兼容性”的涵摄范围更广，“关联性”要求后续的信息处理对于初始目的的严格遵循，可能在一定程度上阻碍大数据产业的发展以及创新型社会的构建。

（二）目的限制原则的法理基础

第二次世界大战结束后，国际社会开始深刻反思战争期间各种非人道的行为，普遍呼吁建立尊重基本人权的法律制度。黑格尔认为，人格的要义在于，我作为这个人，在内部任性、冲动和情欲以及在直接外部的定在等一切方面都完全是被规定了的和有限的，并在有限性中知道自己是某种无限的、普遍的、自由的东西。〔5〕当前，不论英美法系抑或大陆法系，相关制度安排均强调对于个人信息的利用不得以牺牲人格尊严为代价。受社会和他人尊重是人的一种基本需要，是人作为法律关系主体所享有的最基本的人格价值，自然人维护个人信息的准确性、控制个人信息的利用范围是保证个人尊严得到社会认可的体现。〔6〕在“小数据时代”，由于信息收集技术与收集能力普遍处于不发达状态，信息主体尚能有效控制信息是否被处理以及处理的方式，然而，随着大数据技术的突飞猛进，通过个人信息介入个人生活的广度和深度实现了从量变到质变，当个人成为纯粹的“个人信息客体”，被随意监控、分析和操纵，个人的内在决策和外在形象都被控

〔3〕 See Article 29 Data Protection Working Party, Opinion 03 /2013 on purpose limitation 15 (Article 29 Data Protection Working Party 00569/13/EN 2013), p. 21.

〔4〕 参见谢琳：《大数据时代个人信息使用的合法利益豁免》，载《政法论坛》2019 年第 1 期。

〔5〕 参见〔德〕黑格尔：《法哲学原理》，范扬、张企泰译，商务印书馆 2017 年版，第 51 页。

〔6〕 参见张涛：《个人信息的法学证成：两种价值维度的统一》，载《求索》2011 年第 12 期。

制时，个人作为人的完整性和主体地位便已分崩离析，个人的独立和尊严将直接受到挑战。〔7〕为稳固个人的主体性地位，《个人信息保护法》构造了以“人”为中心的制度体系，确保个人对信息的自主性与控制性，目的限制原则即是个人控制体系中重要的组成部分。

目的限制原则要求信息处理者在收集信息时明确告知信息主体信息处理的具体目的，并严格限定后续信息处理的方式，同时给予信息主体同意或反对的权利，能够在一定程度上保障信息主体自主控制信息被以何种方式处理，防止信息处理者以信息主体未能预见到的方式处理信息。自主决定与自愿承担风险是私人自治的重要体现，尊重个人自主决定是否接受信息处理可能造成的风险形塑了个人自治空间，法律对于信息主体真实的意思表示应予尊重，不得任意干涉。作为个人信息的原始所有者，信息主体对于个人信息的收集与利用享有绝对的支配力与控制力，除法律明确规定信息处理的合法性基础外，信息处理者只有在获得信息主体的同意或授权时才能收集或利用信息。目的限制原则要求信息处理者在收集信息阶段应向信息主体详细披露信息处理的方式、可能产生的风险等事项，并承诺在约定的目的范围内处理信息。一般而言，借由信息处理者收集信息时的说明义务，信息主体能够预判让渡信息可能需要承受的风险，并在此基础上作出是否许可他人使用其信息的意思表示。信息主体对于自我信息的控制力与支配力是目的限制原则的理论基础，亦是制约信息处理者尊重目的限制原则的动力来源，只有承认信息主体有权自主决定信息被如何收集与利用，才能促使信息处理者主动寻求信息主体的授权许可。为了获得信息主体的有效同意，信息处理者须将信息处理的目的向信息主体明示，并承诺在约定的目的范围内处理信息，信息处理者超过约定的目的范畴处理信息可能承担违约或侵权责任。

二、大数据时代目的限制原则的现实困境

目的限制原则的效力范围从信息收集开始，及于整个信息处理过程，在包括个人信息的存储、变更、传递与使用等的各个阶段，始终可以发挥其作用。〔8〕目的限制原则这种充足的法律效力力求全面保障信息主体的合法权益，然而在具体实践中，目的限制原则面临以下诸多龃龉。

（一）信息处理目的难以在收集阶段完全确定

目的限制原则要求信息处理的目的应在不迟于信息收集之时予以确定，且目的必须是明确的、合理的。目的限制原则可以有效保证信息主体事先知道信息利用的目的和范围，并能够控制信息收集在事先约定的范围内进行。〔9〕然而，在信息的流转、共享等信息的二次利用成为信息产业普遍遵循的商业运作模式的背景下，传统的目的限制原则受到挑战。目的限制原则依赖于一个前提条件，即信息处理目的在收集信息之时予以确定是可能的，然而大数据分析技术的价值恰恰在于提取隐藏的信息或对信息进行变革性利用，这使得信息处理者无法在信息收集阶段详细阐

〔7〕 参见郭瑜：《个人数据保护法研究》，北京大学出版社 2012 年版，第 84 页。

〔8〕 参见谢永志：《个人数据保护法立法研究》，人民法院出版社 2013 年版，第 57 页。

〔9〕 参见王秀哲：《大数据时代个人信息法律保护制度之重构》，载《法学论坛》2018 年第 6 期。

明信息的所有可能用途。〔10〕于此情形，信息处理者为保障信息处理活动的顺畅进行，倾向于将信息处理目的以一种模糊或宽泛的方式表达出来，导致信息主体无法预期后续的信息处理行为，这种信息的不对称可能引发社会歧视、差别性对待等不公平现象。

目的限制原则要求对于信息的处理必须与信息收集时的初始目的具有直接相关性，反向推之，当信息处理目的与初始目的不一致时，信息处理者应当及时告知信息主体变更目的的缘由并再次征得信息主体的同意。大数据技术的运用使得在信息收集、利用、存储等任何阶段都可能发生信息主体同意信息收集时所未预期的信息处理方式，过于频繁地向信息主体告知变更事项不仅增加了信息处理者的工作负担，也在一定程度上干扰了信息主体的正常生活。此外，目的限制原则植根于私人自治理论，该理论预设信息主体只有充分了解信息处理目的才能决定是否将信息移交给信息处理者。然而，大数据环境中信息处理的复杂性，尤其是自动化决策技术的运用，增加了信息主体理解与选择的难度。实践中，信息主体很少仔细阅读冗长而繁杂的隐私协议，或者囿于自身有限的理性及相关知识的匮乏难以理解具体条款的含义，减损了信息主体同意的有效性。更为重要者，由于信息主体与信息处理者在市场地位、议价能力等方面具有实质不对等性，信息主体即使认识到隐私协议的不合理性也无法要求信息处理者对相关事项予以更正。

（二）忽视了个人信息的利用价值

个人信息所承载的利益形态具有多元性与复杂性，随着大数据处理技术逐渐渗入社会生活各个方面，在日常的人际交往与社会生活中，个人需要不断地与他人交换信息，公务机关与非公务机关亦频繁收集大量信息以改善行政管理或提供更好的服务，社会对于个人信息的客观需求愈益增多。实际上，个人信息不仅与人格尊严及人格自由密切相关，更是相关产业存在和发展的基石，因此不能只关注信息保护，而应将信息保护与信息利用放在同一维度。〔11〕值得肯定的是，立法不再单方面强调信息主体利益的保护，欧盟《一般数据保护条例》（General Data Protection Regulation，GDPR）及我国《个人信息保护法》都开宗明义地指出，应注重信息保护与信息利用之间的平衡。近年来，我国信息产业发展迅速，对个人信息利用的需求也越来越大，大数据分析技术通过结合不同来源的数据可能发现新的趋势、模式和关系，目的限制原则制约了大数据的规模和使用，可能造成经济和社会效益的重大损失。〔12〕根据目的限制原则的逻辑进路，当信息处理目的实现时信息处理者必须尽快删除个人信息，不得留存个人信息，更不得将信息用于其他目的，这严重降低了信息的利用效率，阻碍了信息价值的开发与再利用。从实际层面考量，多数情况下大数据分析所涉及的方法和使用模式是信息处理者以及信息主体在收集信息时没有预料到的，为了遵守目的限制原则，信息处理者必须密切监视处理过程以确保信息处理没有超出约定的范围，然而采取这些措施可能是代价高昂的、困难的甚至是不可能的。〔13〕

〔10〕 See Alessandro Mantelero，The Future of Consumer Data Protection in the E. U. Rethinking the "notice and Consent" Paradigm in the New Era of Predictive Analytics，30 *Computer Law & Security Review*，643－660（2014）.

〔11〕 参见谢远扬：《〈民法典人格权编（草案）〉中"个人信息自决"的规范建构及其反思》，载《现代法学》2019 年第6 期。

〔12〕 See Bart Custers，Helena Ursic，Big Data and Data Reuse：A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection，6 *International Data Privacy Law*，5（2016）.

〔13〕 See Tal Z. Zarsky，Incompatible：The GDPR in the Age of Big Data，47 *Seton Hall Law Review*，1006（2017）.

大数据时代的一个显著特征是，个人信息的价值不再单纯地来自其基本用途而更多源于信息的二次利用，很多信息在收集之时并无意用作其他用途，最终却产生了很多创新性的用途。〔14〕目的限制原则要求信息处理的方式应严格限定于初始目的范围内，不利于新产品、新服务的研发。此外，目的限制原则过于强调信息主体利益的保护，忽视了目的范围之外的信息利用可能造福于社会。2008 年，Google 公司利用用户的搜索关键词成功预测流感爆发趋势即为很好的例证，Google 公司最初收集用户搜索关键词的目的在于改善搜索引擎功能，对于流感趋势的预测显然逾越了 Google 公司收集信息时的初始目的，但毋庸置疑的是，流感趋势预测对于公共卫生部门及时采取防治措施提供了较大帮助。可见，严格的目的限制原则不符合大数据背景下信息多样性利用的现实需求，阻碍了信息经济与信息产业的进一步发展。

三、目的限制原则的改革方案及评价

（一）域外立法变革路径——以欧美为考察对象

目的限制原则最早由美国学者艾伦·威斯汀（Alan Westin）提出，威斯汀主张政府所收集的个人信息只能用于特定目的，不得用于其他目的或者进一步流转，除非提供信息的个人或群体的身份特征已经完全从该信息中移除，或者他们自由地对进一步流转表示同意。〔15〕立法上，目的限制原则可以追溯至 1980 年的《关于隐私保护与个人数据跨境流动的指南》，可以说，欧美国家对于目的限制原则关注的时间较早，积累了丰富的经验，通过考察欧美法的相关规定，可以为我国目的限制原则的优化调整寻求经验借鉴。

为缓和严格的目的限制原则适用上的僵硬性，95 指令规定了“兼容性使用”（compatible use），但并未正面规定“兼容性使用”的具体内涵以及判断标准，以致欧盟国家在评估兼容性时采取了不同的判定标准。具体来说，比利时主要根据信息主体的“合理期待”来判断兼容性，英国和希腊则通过“公平性”（fairness）与“合法性”（lawfulness）衡量兼容性，德国和荷兰则借助于“平衡测试”（balance tests）加以判定。〔16〕2013 年，第 29 条数据保护工作组发布了有关目的限制原则的意见书，明确指出“不同于初始目的的进一步处理并不意味着与初始目的自动地不兼容，在某些情况下，虽然信息的处理与初始目的不同，但二者可能是相符的”〔17〕。关于如何判定“兼容性”，第 29 条数据保护工作组认为应当考虑信息收集目的与信息处理目的之间的关系、信息收集的具体情境与信息主体的合理预期、信息的性质与信息处理对信息主体的影响以及

〔14〕 参见〔英〕维克托·迈尔－舍恩伯格、肯尼斯·库克耶：《大数据时代：生活、工作与思维的大变革》，盛杨燕、周涛译，浙江人民出版社 2013 年版，第 197 页。

〔15〕 参见梁泽宇：《个人信息保护中目的限制原则的解释与适用》，载《比较法研究》2018 年第 5 期。

〔16〕 See Judith Rauhofer, Look to Yourselves, That We Lose Not Those Things Which We Have Wrought: What Do Proposed Changes to the Purpose Limitation Principle Mean for Public Bodies' Rights to Access Third-Party Data, 28 *International Review of Law, Computers & Technology*, 146－147 (2014).

〔17〕 前引〔3〕，第 21 页。

信息处理者采取的保障措施等。〔18〕《一般数据保护条例》承继了第 29 条数据保护工作组关于兼容性使用的判定方式，成为指导欧盟域内判断信息处理是否合乎初始目的的重要依据。有学者认为，虽然相关立法列举了“兼容性”的考量因素，但实践中判定信息处理是否与初始目的相兼容，仍需根据个案具体情境加以判断。〔19〕有学者更是直言，“兼容性评估”在大数据背景下有些抽象和困难，兼容性评估要求考虑信息收集时的具体情境、信息的性质等各种因素，而大数据的运行需要分析不同环境中的数据，使得静态的要素评价几无可能。〔20〕“兼容性使用”作为一个转接通道，为超越初始目的之外的信息利用提供了理论基础，缓和了信息保护与信息利用之间的紧张关系，拓展了信息利用的空间，具有一定的积极意义。然而，“兼容性使用”在判断后续的信息处理是否具有正当性时仍以信息收集时的初始目的为基点，忽视了时间、环境等外在因素的变迁可能导致信息处理目的的更迭。2017 年，第 108 号公约协商委员会主张，不应以信息主体可能认为无法预料的、不适当的或令人反感的方式处理信息，将信息主体暴露于不同的风险或比初始目的所预设的更大的风险，可以视为以无法预料的方式处理信息。〔21〕指南改变了欧盟一直以来所遵循的目的限制原则的调整思路，为目的限制原则在新时代背景下的灵活运用开辟了新的方向，遗憾的是，指南仅具有参考性意义，不具有强制的法律效力。

不同于欧盟立法，美国主要通过场景规则的构建来改革目的限制原则所面临的困境，场景规则的提出与美国隐私概念的不确定性有关，自 1890 年沃伦（Samuel D. Warren）与布兰迪斯（Louis D. Brandeis）提出隐私这一概念以来，理论界关于隐私的具体内涵一直存在争议。在此背景下，美国学者海伦·尼森鲍姆（Helen Nissenbaum）提出了场景完整性理论（contextual integrity theory），主张隐私的保护应与特定情境联系起来，信息的收集和传播应当符合具体情境并遵守特定情境下的相应规则，隐私是否受到侵害需要综合考量具体场景下的多种因素。〔22〕场景完整性理论由于其强大的包容性与灵活性得到立法者的青睐，2012 年，白宫在一份文件中明确提出“尊重场景原则”（respect for context principle），消费者有权期待企业收集、使用以及披露个人数据的方式与其提供数据时的场景相一致。〔23〕与此同时，联邦贸易委员会强调在符合一定场景下企业可以直接收集或使用消费者信息而无需征得消费者的同意，除非企业以信息收集时所声称的实质性不同的方式使用信息或出于某些目的而收集敏感信息。〔24〕2018

〔18〕 参见前引〔3〕，第 23－26 页。

〔19〕 See Bert-Jaap Koops, The (In) Flexibility of Techno-Regulation and the Case of Purpose-Binding, 5 *Legisprudence*, 179 (2011).

〔20〕 See Tal Z. Zarsky, Incompatible: The GDPR in the Age of Big Data, 47 *Seton Hall Law Review*, 1008 (2017).

〔21〕 See Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data, available at https://rm.coe.int/16806ebe7a, last visited on May 27, 2021.

〔22〕 See Helen Nissenbaum, Privacy as Contextual Integrity, 79 *Washington Law Review*, 136－157 (2004).

〔23〕 See See White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, available at https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf, last visited on Aug. 20, 2021.

〔24〕 See Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid change, March. 2012, available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, last visited on Jul. 19, 2021.

年，《加州消费者隐私法案》（California Consumer Privacy Act，CCPA）吸收了“尊重场景规则”，法案明确“若个人信息的处理符合信息收集时的具体情境，则认为信息处理行为是合理的、适当的”〔25〕。“尊重场景规则”主张不应严格固守信息收集时的初始目的，若后续的信息处理符合信息收集时的具体场景则判定信息处理行为是合法的，但“场景”具有流动性与易变性，不利于当事人合理预期的形成。有鉴于此，2020 年的《加州隐私权法案》（The California Privacy Rights Act，CPRA）对目的限制原则进行了调整，采取“初始目的”与“场景路径”双重认定模式，其规定“企业收集、使用、存储、共享消费者个人信息应当是合理的、必要的，并且与信息收集时的初始目的相符，或具有与信息收集时的情境相适应的其他披露目的”。易言之，若个人信息的后续处理与初始目的或信息收集时的场景相符，就应当认定为正当的信息处理行为。

（二）理论界的改革方案

大数据环境下，目的限制原则暴露出来的弊端愈来愈多，学界对此进行了反思并提出不同的改革方案。“合法利益测试说”认为“目的限制原则”已经无法适应社会发展的需要，应当评估为实现某项合法利益可以在何种程度上正当化信息处理行为，以此决定信息处理行为是否妥当。〔26〕“扩张解释目的说”主张综合考量信息收集时的情形、信息的性质以及信息处理对信息可能造成的后果等因素，来扩张解释信息收集时初始目的，禁止任何逾越初始目的的信息利用行为。〔27〕“风险限定说”建议融入场景与风险的理念，以“风险限定”替代“目的限定”，亦即处理个人信息不能引发高于原有程度的、用户无法预期的风险。〔28〕风险限定论认为，判定信息的利用是否具有正当性关键在于信息处理是否引发了不合理的风险，这种不合理的风险包括精神压力、差别待遇、人身财产损害的可能性以及是否符合信息主体的预期与信息披露时的情境。〔29〕

关于前述改革方案，“合法利益测试说”的观点较为激进，其认为应当彻底放弃“目的限制原则”的基础性地位，主张以“合法利益”作为信息处理是否具有正当性的唯一判断标准，如果信息处理是为实现某项合法利益所必需，则该信息处理具有妥适性，反之则否。“合法利益测试说”在一定程度上缓和了后续信息处理受限于初始目的的局限性，能够为实践中信息处理的适时变动提供理论依据。然而，“合法利益”是模糊且抽象的法律概念，其具体内涵及外延有待于个案情境中予以判定，由此可能导致不同主体对于“合法利益”存在不同的解释，无法为司法实践提供明确的指导。从实际层面考量，信息主体由于信息不对称、专业能力的匮乏等现实因素很难举证证明信息处理者所声称的“合法利益”是否合理，可能致使“合法利益测试”异化为强势地

〔25〕 The California Consumer Privacy Act of 2018 （CCPA），available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121，last visited on Jul. 11，2021.

〔26〕 See Lokke Moerel，Corien Prins，Privacy for the Homo Digitalis：Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things，available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123，last visited on Apr. 23，2021.

〔27〕 参见前引〔15〕，梁泽宇文。

〔28〕 参见范为：《大数据时代个人信息保护的路径重构》，载《环球法律评论》2016 年第 5 期。

〔29〕 参见李媛：《大数据时代个人信息保护研究》，华中科技大学出版社 2019 年版，第 200 页。

位的信息处理者肆意处理他人信息的辩护工具。“扩张解释目的说”避免了后续信息处理溢出初始目的范围可能面临的“目的落空”之诘问，保障了“初始目的”存在的价值，但其通过采取综合考量模式来扩张解释信息处理的初始目的不仅不合理地改变了原本意义上的“目的”，还在一定程度上淡化了目的明确性，导致当事人无法产生合理的预期。需明确的是，个人信息保护并非旨在保护信息本身不被收集、利用，而是保护信息主体免受信息处理可能造成的伤害，严格限制信息的收集而放松信息的利用不符合时代发展趋势。“风险限定说”不要求信息处理者对于初始目的的严格遵循，只要信息处理者将信息处理可能引发的“风险”控制在合理范围之内就可以自由处理信息，符合实践中多元化的信息利用需求。然而，罔顾信息收集时的初始目的，不利于信息主体合理预期的形成以及社会的有序发展。

四、个人信息的类型化分析

（一）个人信息类型化的必要性

1. 个人信息固有的差异性

个人信息范围广泛、种类繁杂，不同的个人信息与自然人的关联性是不同的，面对丰富庞杂的个人信息集群，统一个人信息的保护模式忽视了个人信息的差异性及其对个人的影响程度，因此，区分规制个人信息从而提供更为细致的保护实乃现实必需。

司法实践中，法院首先认为信息的内容决定信息处理风险的高低，如果所涉信息的内容是普通个人信息，则诉请通常不会得到法院的支持，但如果相关的个人信息涉及当事人的隐私，或者个人信息属于敏感事项，那么相关的诉请就有很大的可能获得法院的支持，因此，只有对受保护的个人信息进行类型化处理，才能“避免个人信息概念的模糊性缺陷，防止规范适用的空洞化”〔30〕。个人信息固有的差异性要求我们对不同个人信息给予不同程度的保护，这是平等原则的内在要求，平等并非意味着忽视个人信息的差异性刻意追求均等化保护。平等原则包括两重含义：平等的必须平等对待，不平等的必须不平等对待。这意味着平等原则不仅仅允许差别的存在，而且允许差别对待。〔31〕个人信息之间天然地存在差异，不加区分地对所有个人信息实行同等保护，违背了平等原则的实质内涵。

2. 促进信息市场有序发展

历史上，无数次思想启蒙与思想解放运动的经验告诫我们，人类从愚昧无知走向文明发展的关键就在于信息的获取与利用。目前，信息的共享与流通已成必然趋势，信息壁垒逐渐被打破，任何阻碍或隔绝信息流通的行为都是违背社会实际发展现状的。信息时代对于个人信息利用的内在需求要求我们必须摒弃传统的只关注于信息主体利益的滞后观念，适度地释放信息的经济价值才能有利于社会的有序发展。在信息处理过程中，信息主体的利益与信息处理者的利益处于持续

〔30〕 前引〔11〕，谢远扬文，第 146 页。

〔31〕 参见〔德〕伯恩·魏德士：《法理学》，丁小春、吴越译，法律出版社 2003 年版，第 165 页。

的博弈之中，过于强化信息主体利益的保护，必将侵蚀信息的合理利用空间；反之，偏重信息处理者的利益，则势必影响信息主体的利益。

大数据时代，信息经济已成为我国市场经济发展的重要组成部分，个人信息一体化的保护模式增加了信息处理者处理信息的顾虑，信息处理者可能因惧怕动辄承担法律责任而放弃信息产品的研发与升级，这对于我国信息产业的长足发展是不利的。从成本收益的角度分析，统一保护模式虽然使公民信息得到了绝对的保护，但国家为此投入了大量成本，包括司法成本、社会成本等，总体上无益于社会效益的增加，因而并非是最优的资源配置方式。〔32〕

（二）个人信息类型化的路径选择

1. 个人信息类型化的理论尝试与规范应对

关于个人信息的类型化区分，我国理论层面与规范层面存在不同的观点，就理论层面来说，可谓众说纷纭，以下简要概述。有学者依据个人信息与人格关系的紧密程度将个人信息区分为人格紧密型个人信息和人格疏远型个人信息，凡符合直接识别性、敏感性、个体性强三个特征之一的个人信息即为人格紧密型个人信息，反之则为人格疏远型个人信息。〔33〕还有学者立足于个人信息生命周期及其在不同周期阶段呈现的利益形态，将个人信息划分为个人私密信息、个人事实信息以及个人预测信息。〔34〕还有学者将个人信息划分为自然性个人信息与社会性个人信息，自然性个人信息是信息主体与生俱来且无法轻易改变的信息，社会性个人信息是信息主体为了社会生活所必须而由个人主动或被动地获取的相应符号或信息。〔35〕由上述不完全列举可知，我国学者在个人信息类型化问题上各执己见，但其区别规制个人信息的意旨均在细化个人信息的保护方式，并在此基础上平衡信息主体与信息处理者的利益。

就规范层面来说，截至目前，我国诸多规范均对个人信息的类型化予以了明确规定。2012年发布的《信息安全技术 公共及商用服务信息系统个人信息保护指南》第3.2条明确表示“个人信息可以分为个人敏感信息和个人一般信息”。《民法典》第1034条第3款依据信息的私密性将个人信息区分为私密信息与非私密信息，第1036条则根据公开与否将个人信息区分为已经合法公开的个人信息与未公开的个人信息。新近颁布的《个人信息保护法》延续了区别规制个人信息的立法理念，将个人信息区分为个人一般信息与个人敏感信息以及已公开的个人信息与未公开的个人信息。可见，我国立法对于个人信息的类型化存在不同的规定，由此引发的问题是，不同类型化的个人信息之间可能存在交叉重叠之处，例如，性取向可能同时属于个人敏感信息、私密信息以及非公开个人信息，此时应当选取何种保护路径不仅关系当事人合法权益的保护，还关系法律体系的内在协调。

---

〔32〕 参见董悦：《公民个人信息分类保护的刑法模式构建》，载《大连理工大学学报（社会科学版）》2020年第2期。

〔33〕 参见项定宜、申建平：《个人信息商业利用同意要件研究——以个人信息类型化为视角》，载《北方法学》2017年第5期。

〔34〕 参见袁泉、王思庆：《个人信息分类保护制度及其体系研究》，载《江西社会科学》2020年第7期。

〔35〕 参见刘迎霜：《大数据时代个人信息保护再思考——以大数据产业发展之公共福利为视角》，载《社会科学》2019年第3期。

2. 个人信息类型化的理想选择

上述个人信息类型化的学说有一定的说服力，但都不足以成为重构目的限制原则的根本性的类型划分。笔者认为，以信息的敏感度将个人信息区别为个人一般信息与个人敏感信息进而对目的限制原则采取不同的解释路径，能统筹兼顾信息主体利益与信息处理者利益，实现信息保护与信息利用之间的动态平衡。根据《个人信息保护法》第 28 条之规定，“敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息”。可见，个人敏感信息与个人一般信息的区分触及了个人信息保护实质意义上的差异性，较之于个人一般信息，侵害个人敏感信息对信息主体造成的损害更为严重，因而需要对其予以更严格的保护。

此外，以个人敏感信息与个人一般信息的区分来构建个人信息保护规范体系符合国际立法趋势，也契合了我国的立法规范。目前，比较法上大多国家和地区采取区别规制个人敏感信息与个人一般信息的立法体例。例如，1981 年欧洲理事会颁布的《关于个人数据自动化处理的个人保护公约》、2018 年生效的《欧盟一般数据保护条例》、2018 年日本修正的《个人信息保护法》等。我国规范层面，《民法典》《个人信息保护法》《征信业管理条例》以及《信息安全技术 公共及商用服务信息系统个人信息保护指南》《信息安全技术 个人信息安全规范》等诸多规范性文件或直接或间接规定了敏感信息。司法实践中，法院亦认为应当对于敏感信息予以特殊对待。在“罗某与巢某土地登记纠纷”一案中，法院认为，合法权利人对于房屋相关权属信息为个人敏感信息，在非法定情形下，未经权利人同意不应公开。〔36〕在“朱烨与百度网讯科技公司隐私权纠纷”一案中，法院认为，将个人信息区分为个人敏感信息和非个人敏感信息的一般个人信息而允许采用不同的知情同意模式，能够在保护个人人格尊严与促进技术创新之间寻求最大公约数。〔37〕可以说，个人敏感信息与个人一般信息的区别规制能够成为我国个人信息分类保护的基础性框架，是适合于我国个人信息类型化保护的理想的路径选择。

五、类型化视角下目的限制原则的重构

（一）个人敏感信息：禁止目的外利用

个人敏感信息与信息主体的人格尊严以及人格自由密切相关，非法收集或不当利用敏感信息可能对信息主体的人身权益造成严重损害，这种损害不局限于隐私侵害，而是包括财产损失、歧视性待遇、精神伤害等在内的各种形式的物质性以及非物质性损害。处理敏感信息具有高度的危险性，因而在处理敏感信息时应当恪守目的限制原则，禁止超越初始目的范围处理敏感信息。

〔36〕 参见江苏省南京市中级人民法院（2020）苏 01 行终 480 号行政判决书。

〔37〕 参见江苏省南京市中级人民法院（2014）宁民终字第 5028 号民事判决书。

如前所述，收集个人敏感信息必须具有明确、合理的目的，其中“合理性”的判定涉及价值层面冲突关系的利益衡量，可以借助于公法上的比例原则进行判定。比例原则缘起于德国警察法，后发展为公法领域的“帝王条款”，比例原则内含三个子原则，即适当性原则（Geeignetheit）、必要性原则（Erforderlichkeit）及狭义比例原则（Verhltnismigkeit im engeren Sinne）。〔38〕近年来，比例原则在我国呈现出不断扩张的趋势，不仅行政法、刑法等公法领域强调比例原则的指导价值，私法领域也逐渐认可比例原则的作用空间，更有学者主张比例原则应当作为民法的一项基本原则，强调比例原则在私法领域的普适性。〔39〕比例原则作为方法论意义上的工具性原则，〔40〕考察的是目的与手段之间是否均衡，处理敏感信息是否具有“合理性”亦在评价信息处理者的处理行为与其所意愿达成的目的之间是否合理，与比例原则内蕴的价值取向具有一致性。此外，比例原则内含的三个子原则呈现阶层式的构造，在具体适用上具有严格的顺序限制。比例原则的阶层式构造以及顺序判断模式提供了精致的分析工具，使得“合理性”的判定既不过于空洞也有章可循。具体来说，适当性原则要求信息处理者的行为应当有助于合法利益的实现，此处的“合法利益”应作广义的解释，不仅包括法律明确规定的正当性利益，还包括法律虽然没有明确规定但从规范目的可推导出的合法性利益。需注意的是，适当性原则要求信息处理者的行为具有实现合法权益之可能性即可，并不要求该合法利益必须真切地实现，由于事物的普遍联系性，客观上有利于实现合法利益的信息处理行为可能无限绵延，行为的作用力大小亦不相同，但不得将过于遥远的作用力纳入合理性范畴，否则可能堵塞信息主体获取救济的途径。必要性原则要求信息处理者在处理敏感信息时必须选择对信息主体侵害最小的处理措施，且所采取的措施必须具有经济性与便利性，若实现该信息处理目的成本过高，应否定信息处理行为的合理性。均衡性原则要求处理敏感信息可能对信息主体利益造成的损害应当与所要实现的目的具有相称性，不能显著失衡，相称性内蕴多元的价值评价，需要在具体个案中综合考量。

（二）个人一般信息：适度允许目的外利用

大数据时代，个人的生活交往以及社会的存续发展离不开个人信息的收集与利用，对于与信息主体联系不甚紧密的个人一般信息，应更多关注于其在社会生活中的流转与利用，原则上来说，信息处理者必须谨遵目的限制原则，但为满足社会对于信息利用的需求，应当允许信息处理者在一定条件下超越初始目的范围利用信息，前提是不得给信息主体造成不合理的风险。

现代社会是风险社会，各种各样的风险无处不在。贝克认为，风险的概念直接与反思性现代

〔38〕 Vgl. Landessozialgericht Hamburg. Begrenzung der Erlschenswirkung bei Nichtanzeige einer Beschftigung，2006 Heft 1，S. 18.

〔39〕 参见郑晓剑：《比例原则在民法上的适用及展开》，载《中国法学》2016 年第 2 期；纪海龙：《比例原则在私法中的普适性及其例证》，载《政法论坛》2016 年第 3 期。

〔40〕 See Aharon Barak，Proportionality，Constitutional Rights and Their Limitations，Cambridge University Press，2012，p. 131.

化的概念相关，风险可以被界定为系统地处理现代化自身引致的危险和不安全感的方式。〔41〕还有学者认为，风险是某种不可预见情形出现的可能性，其可能是自然事件或人类活动的结果，也可能是两者共同作用的结果。〔42〕可见，“风险”一词具有多重面向，其在不同语境中具有不同的含义。个人一般信息更多体现为信息利用价值，因此不宜片面强调信息处理对于初始目的的严格遵循，而应要求信息处理者将信息处理可能引发的风险控制在合理范围之内，以符合大数据时代信息多元利用的趋势。一般来说，影响信息处理风险程度的因素主要有以下几项：第一，信息的敏感性程度。个人信息的核心特征在于识别性，识别包括直接识别与间接识别，直接识别指通过该信息可以直接确认某一自然人的身份，间接识别指通过该信息虽然不能直接确认某人的身份，但可以结合其他信息加以确定。〔43〕个人信息的此种特性决定了个人信息的范围具有广泛性与动态性，具体个案中，如果信息的敏感度越高，则信息处理行为受到的限制越多。第二，信息处理者的风险控制能力。特定的行为或活动与特定的风险相联系，当行为人以其行为开启一定的风险或者维持一定的风险状态时，该风险实现时则行为人难辞其咎。〔44〕通常来说，信息处理活动产生的风险是由信息处理者制造的，信息处理者在享受信息处理带来利益的同时亦负有合理控制风险的义务。风险实现的可能性以及风险的严重性与信息处理者控制风险的能力密切相关，信息处理者控制风险的能力越强，则风险发生的可能性越低、风险的严重性亦越低。第三，信息主体的预见能力。合理的信赖受法律保护，信息处理者不得以信息主体基于信息收集时的初始目的所无法预期的方式处理信息。〔45〕信息处理者对于信息主体信赖其以约定方式利用信息的合理预期负有保护义务，不得无故使信息主体的合理预期落空，否则有碍于构建良性的信息处理环境，若信息处理产生的风险高于信息主体的合理预期则为法律所不允许，信息处理者需将相关风险告知信息主体并重新获得信息主体的授权同意。须注意的是，即使信息处理产生的风险在合理范围之内，但信息主体明确表示拒绝接受信息处理的，信息处理者亦不得继续处理信息，除非信息处理者有证据证明信息处理的利益大于信息主体的利益。

六、结　语

法律需要稳定，但不能一成不变，所有关于法律的思考都是在努力调和稳定与变化这两种相互冲突的需求。〔46〕目前，大数据技术渗透到社会生活的各个方面，信息科技的快速变革要求个人信息保护理念应从严格限制信息收集转向平衡兼顾信息保护与信息利用，传统的目的限制原则

〔41〕 参见〔德〕乌尔里希·贝克：《风险社会》，何博闻译，译林出版社 2004 年版，第 19 页。

〔42〕 参见〔英〕罗伯特·鲍德温、马丁·凯夫、马丁·洛奇编：《牛津规制手册》，宋华琳等译，上海三联书店出版社 2017 年版，第 348 页。

〔43〕 参见黄薇主编：《中华人民共和国民法典人格权编解读》，中国法制出版社 2020 年版，第 209 页。

〔44〕 参见叶金强：《风险领域理论与侵权法二元归责体系》，载《法学研究》2009 年第 2 期。

〔45〕 See Dag Elgesem, The Structure of Rights in Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of Such Data, 1 *Ethics & Information Technology*, 283 - 287 (1999).

〔46〕 See Roscoe Pound, Interpretations of Legal History, Cambridge University Press, 1967, p. 1.

无法有效应对社会的发展变化，有必要对其加以修正。

个人信息种类繁杂，不同个人信息与信息主体的紧密程度差异甚大，统一的个人信息保护模式无法合理兼顾信息保护与信息利用之双重价值目标，类型化构建个人信息保护制度实有必要。具体而言，由于个人敏感信息关系信息主体基本的人格尊严，在处理敏感信息时必须恪守目的限制原则，禁止恣意扩大初始目的应有的范围，而对于个人一般信息，可以适度允许超越初始目的范围的信息利用行为，但不得超过信息收集时信息主体能够合理预期的风险。我国《个人信息保护法》虽然规定了目的限制原则，但基本沿用传统的保护路径，存在不足之处，应适度调整目的限制原则的内涵以期助力我国信息产业与信息社会的有序发展。

Abstract：As the basic principle of personal information processing，the purpose limitation principle requires that information processing activities shall not overflow the scope of the original purpose at the time of information collection，which guarantees the subject of the information independent control and dominate over personal information. However，in the era of big data，the diverse use of information is becoming more and more normal，and the purpose of information processing is difficult to be fully determined at the information collection stage. Besides，the strict purpose limitation principle ignores the use value of personal information. Information protection and information utilization are both value goals pursued by the law，and we can't ignore one and lose the other. Therefore，it is necessary to reshape the connotation of the purpose limitation principle from the perspective of personal information typology. In other words，when dealing with personal sensitive information，we must strictly abide by the purpose limitation principle，and processing beyond the scope of the original purpose is prohibited. In principle，the processing of personal general information must also comply with the purpose limitation principle，but under special circumstances，it is allowed to process information beyond the initial purpose，provided that it shall not cause risks higher than expected by the subject of personal information.

Key Words：the purpose limitation principle，information protection，information utilization，personal sensitive information，the risk limitation

（责任编辑：王叶刚　赵建蕊）

财经法学 No. 2，2022
pp. 54 - 68

数字防疫中个人信息治理的“链”“法”协同机制研究

胡元聪　龚家锋*

内容提要：在本次疫情防控中，人工智能、大数据等数字技术在降低疫情传播风险的同时使个人信息治理面临新的风险。联盟链近年来在诸多领域得到广泛应用，成为化解数字防疫中个人信息治理风险的可行工具。但在应用联盟链治理风险的同时，还需要对相应制度予以优化，从而在技术迭代与制度优化的作用下实现联盟链与法律的“携手共治”。对此，应当消除联盟链与法律之间的张力，进而构建以法律治理为主、以联盟链治理为辅的“链”“法”协同机制。具体而言，通过构建与法律相匹配的联盟链治理机制及与联盟链相适应的法律治理机制，融合区块链技术和法律各自的优势，以此来提升“链”“法”协同机制在数字防疫中个人信息治理方面的能力，从而提高国家治理现代化水平。

关键词：数字防疫　个人信息治理　风险治理　联盟链　“链”“法”协同

一、研究背景与问题的提出

新型冠状病毒肺炎疫情（以下简称“疫情”）自暴发以来，即在全球迅速蔓延。预计到世界范围内的新冠肺炎疫苗普遍接种前，我国仍将长期处于“外防输入，内防扩散”的常态化疫情防控中。与之前历次突发重大公共卫生事件相比，本次疫情防控的最大特点是“将云计算、大数据、人工智能等新兴技术应用于疫情监测分析、人员流动和社区管理等联防联控的各个方面”〔1〕进

* 胡元聪，西南政法大学经济法学院教授、西南政法大学中国市场经济法治研究中心主任；龚家锋，西南政法大学人工智能法律研究院助理研究员。

本文为国家社科基金重点项目“人工智能研发与应用风险治理的财税法协同机制研究”（21AFX021）、重庆市研究生科研创新项目“疫情防控中个人信息保护的区块链技术进路研究”（CYS20152）的阶段性成果。

〔1〕《工业和信息化部办公厅关于运用新一代信息技术支撑服务数字防疫和复工复产工作的通知》，载 http://www.gov.cn/zhengce/zhengceku/2020-02/19/content_5480843.htm，最后访问时间：2021年1月17日。

行数字防疫。〔2〕但数字技术的不确定性和规制数字技术制度的不确定性导致疫情防控“危”“机”并存：通过对公民个人信息〔3〕的治理〔4〕进行数字防疫，一方面有效地降低了疫情传播风险，另一方面却使公民个人信息面临治理风险。易言之，数字技术为降低疫情传播风险而应用，但数字技术的应用又使个人信息治理产生了新的风险。如何消除数字防疫和个人信息治理之间的冲突龃龉问题以化解个人信息治理之“危”进而利用数字进行防疫之“机”，是数字防疫亟须解决的问题。

具体来讲，随着数字技术的不断应用，越来越多的部门开始大规模搜集和使用个人信息进行分析，与此同时，一些“不当利用个人信息的侵权行为愈发普遍”〔5〕。部分防疫部门实行“地毯式”搜查却可能疏于管理，一些有关疫情的图片、视频和数据等充斥于社交平台，部分确诊或疑似患者的个人信息在网络上广泛流传。在各地推出健康码、行程卡等应用程序和基层登记办法后，大量个人信息既留存于网页、应用程序等数字代码中，也广泛暴露在商超、银行等公共场所入口的纸质登记簿上。这使得为数字防疫而搜集的个人信息产生了治理风险。不同于传统商业领域的个人信息侵害行为，数字防疫搜集的个人信息搜集面广、覆盖人群多。不当利用行为不仅“侵犯了公民的个人隐私权益，可能成为下游犯罪的预备条件”〔6〕，而且增添社会恐慌情绪，给数字防疫增加阻力，甚至“可能危害国家政治安全与社会安全”〔7〕。

区块链技术具有去中心化、可溯源的特点，经过数年的研发创新，已针对不同的应用领域衍化出公有链、联盟链等多种类型。其在业界担忧的去中心化、总量、算力、跨链方面不断改进，〔8〕可能在全球范围内引起新的技术和产业变革〔9〕。我国已逐渐成为区块链技术大国，区块链专利数量位居世界前列。联盟链成为我国区块链技术应用的趋势，其在金融、政府治理、产品溯源等方面多有实践。习近平总书记强调，要发挥区块链技术在促进信息共享、提升协同效率等方面的作用，推进区块链和经济社会融合发展。〔10〕我国《“十四五”规划和2035年远景目标纲要》也提出要以联盟链为重点发展区块链服务平台和应用方案。具体在数字防疫的个人信息治理方面，联盟链在疫情防控和个人信息治理中均已有相关应用：如济南的“区块链＋疫情防控”〔11〕系统、

〔2〕本文所称“数字防疫”是云计算防疫、大数据防疫和人工智能防疫的总称。

〔3〕本文所称“个人信息”是指《中华人民共和国民法典》第1034条规定的个人信息，即以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

〔4〕依照《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）第4条的规定，个人信息的处理包括个人信息的收集、储存、使用、加工、传输、公开等活动。本文所称“个人信息治理”主要是指对个人信息处理行为进行规范的活动。

〔5〕孙莹：《大规模侵害个人信息高额罚款研究》，载《中国法学》2020年第5期，第106页。

〔6〕叶名怡：《个人信息的侵权法保护》，载《法学研究》2018年第4期，第88页。

〔7〕《总体国家安全观视角下个人信息保护机制研究》，载http://www.gjbmj.gov.cn/n1/2020/0509/c411145-31702913.html，最后访问时间：2021年1月19日。

〔8〕参见《利用区块链促进税收管理现代化的研究》课题组、张国钧等：《基于区块链的“互联网＋税务”创新探索——以深圳市税务局的实践为例》，载《税务研究》2019年第1期。

〔9〕参见中国区块链技术和产业发展论坛：《中国区块链技术和应用发展白皮书（2016）》。

〔10〕参见《习近平主持中央政治局第十八次集体学习并讲话》，载http://www.gov.cn/xinwen/2019-10/25/content_5444957.htm，最后访问时间：2021年1月19日。

〔11〕《济南全国首发“区块链＋疫情防控”标准》，载http://www.jinan.gov.cn/art/2020/4/10/art_1861_4197790.html，最后访问时间：2021年1月19日。

广州南沙的“疫情防控协同系统”〔12〕等，积极利用联盟链防控疫情；再如中国人民银行主导的“征信链”，利用联盟链确保包括个人信息在内的信用信息安全并推动信息共享〔13〕。此外，联盟链的技术特征与《个人信息保护法》的“信息保护义务”以及数字防疫中政府部门居中管理调度的要求相契合。基于此，本文拟探讨以下四方面的问题：数字防疫对个人信息治理产生了哪些风险，联盟链能否成为化解这些风险的工具，如何处理联盟链和法律在数字防疫中个人信息治理的关系，怎样构建全方位的数字防疫中个人信息治理“链”“法”协同机制。

二、数字防疫中个人信息治理面临的风险

在本次疫情防控中，大数据、人工智能等数字技术筑起了一道道防疫“数字长城”。但受技术特性和应用实践的限制，数字技术给个人信息治理带来了技术风险和制度风险。具体表现在以下三个维度：

（一）个人信息数量激增，挑战防控信息真实性

在本次疫情防控中，政府利用电信企业的通信信息配合其他实名制信息建立了健康码、行程卡等防疫工具。这些工具可以动态跟踪人员流向，从而有效降低疫情传播风险。与此同时，需要处理的个人信息迎来“数据核爆”。以北京“健康宝”为例，其以个人信息和通信信息为基础，出入公共场所必须校验个人“健康宝”信息。这一特殊工具为有效防控疫情、排查人员流向发挥了巨大作用，同时在短时间内产生了海量信息。其自上线以来，使用人数和查询次数激增，后台所需存储的对应信息量持续增高。截至 2021 年 8 月 13 日，其累计查询、使用次数达 79 亿次。〔14〕信息的真实性是数字防疫中个人信息治理的前提。如果不能及时处理激增的个人信息，便会出现挑战防控信息真实性的风险，从而动摇防控信息的真实性基础。“个人信息是大数据和人工智能的原料。”〔15〕激增的海量个人信息具有多样性、价值性和快速性的特点，这就要求防疫部门具备高水平的信息治理能力，以保障数字防疫基础信息的真实性。这对于习惯传统治理模式的各级防疫部门而言可能是一个不小的挑战。部分防疫部门因为防控压力激增，忙于落实防控要求，可能来不及处理激增的海量涉疫信息，进而会影响到防控信息的真实性。同时，个别防疫部门出于政绩考虑或防控压力，主观上可能有漏报、瞒报行为，或者选择性收集对自己有利的信息，这也容易挑战防控信息真实性进而影响到数字防疫的准确性。

（二）个人信息安全危殆，影响防控信息公信力

个人信息安全受到威胁的主要原因在于第三方的处理：若信息只在两个主体间传输，二者对信息的加工、处理涉及的安全问题通常有相关的合意，此时一般不易出现安全风险。但如果不能

〔12〕《打通防疫“数据烟囱”，广州南沙防疫信息化系统上线》，载 http://zfsg.gd.gov.cn/xxfb/dsdt/content/post_2883625.html，最后访问时间：2021 年 1 月 19 日。

〔13〕 参见《科技赋能金融，“链”上无限可能》，载 https://www.thepaper.cn/newsDetail_forward_14441734，最后访问时间：2021 年 10 月 10 日。

〔14〕 参见《北京市新型冠状病毒肺炎疫情防控工作新闻发布会（第 240 场）》，载 http://www.beijing.gov.cn/shipin/Interviewlive/514.html，最后访问时间：2021 年 11 月 7 日。

〔15〕 王成：《个人信息民法保护的模式选择》，载《中国社会科学》2019 年第 6 期，第 125 页。

在涉及第三方处理时实现可溯源，信息就容易被进一步转手并泄露。如在数字防疫中，个人信息往往辗转于多个防控主体之手。频繁的转移为恶意攻击提供了难得的机会，〔16〕出现安全风险在所难免。同时，数字防疫搜集的海量个人信息储存在传统中心化服务器中，通过开放的互联网传输和整合。信息可能没有时间标识，复制成本低，存在较大的泄漏及篡改风险。而常规信息加密方法只能在一定程度上缓解安全风险，并不能彻底防范外部攻击，无法根本解决个人信息的安全问题。信息的安全性及公信力是数字防疫中个人信息治理的根基。如果不能保证数字防疫中个人信息安全，便会出现影响防控信息公信力的风险，进而可能影响到数字防疫的权威。涉疫个人信息一旦被泄漏或篡改，配合防疫的公民隐私便暴露在公众的视线下，将使公民承受巨大的心理和舆论压力。这将影响公民填报信息的积极性并降低其对防控的信任度，进而影响到防控的效率、精度以及防控信息的公信力。以北京“健康宝”为例，其由公权力机关负责运营并受到多重技术保护和严格监管，却也出现了个人信息泄露事件：不法分子在网络上低价售卖大量明星的“健康宝”照片、身份证号码、核酸检测结果等相关个人信息。〔17〕不同于涉疫信息表格、截图、流调报告等泄露事件，该事件源自公共防疫应用程序。即使事故由技术服务商的程序漏洞而非政府的原因引起，也可能使防控信息的公信力受损。

（三）个人信息孤岛阻隔，降低防控信息共享度

“信息孤岛”是指信息被不同的主体储存，因储存、传输标准不统一或缺乏交流渠道等原因成为相互独立的数据集，而无法分享、整合的情形。在数字防疫中，个人信息控制主体众多，仅笔者就接触到三类：其一是基于法律法规授权的主体，如政府、医院等；其二是基于日常业务而成为信息控制者的主体，如电信企业、航空公司等；其三是处于模糊地带的主体，如商场、银行等需要统计人员流向的公共场所。每个信息控制主体都有各自的信息管理系统，信息控制主体之间相互独立，无法共享各自控制的信息。虽然近年来各界对破解“信息孤岛”提出了诸多观点并付诸实践，但受硬件设备和沟通渠道的限制，数字防疫中的“信息孤岛”现象仍然存在。信息的共享度是数字防疫中个人信息治理效率的衡量标准之一。如果不能解决“信息孤岛”问题，便会出现降低防控信息共享度的风险，从而降低防疫协同效率。个人信息控制主体本应相互配合，实现多向信息共享，减少不必要的重复步骤以提升效率。但实践中部分防疫部门仍在一定程度上各自为政，一些信息可能没有及时共享。以 2021 年春节地方政府为落实“就地过年”而排查外地返乡人员为例，部分相同的个人信息因缺乏共享而被多次重复统计。〔18〕在冬季部分地区疫情发散的背景下，各地面临严峻的防控形势。多次重复统计个人信息符合防控形势需要。但相同的个人信息因缺乏共享而被不同的防疫部门多次重复统计，一定程度上提高了防控成本并降低了防控效率。如果防疫部门之间加强信息共享，减少不必要的重复步骤，起码不再要求已经排查过的人员重复填报其他部门已经登记过的信息，则可以在一定程度上加快排查速度，提高信息的利用

〔16〕 参见邢会强：《论数据可携权在我国的引入——以开放银行为视角》，载《政法论丛》2020 年第 2 期。

〔17〕 参见《多名艺人“健康宝照片”遭泄露》，载 https://mp.weixin.qq.com/s/D198CIQsh_R5jaNdFiXeJQ，最后访问时间：2021 年 1 月 19 日。

〔18〕 仅笔者春节返乡就接触到五次统计，其中部分统计内容相同：其一是公民主动上报及相互检举；其二是社区等基层人员逐户排查上报；其三是教育部门统计学生返乡信息；其四是公安部门利用交通实名信息统计；其五是电信、互联网公司等对其用户流向进行分析。

效率。

三、数字防疫中联盟链应用于个人信息治理的可能性

个人信息的处理是数字防疫的必然要求，但数字防疫又给个人信息治理带来了新的风险。联盟链可以为数字防疫中的个人信息治理提供新的思路。联盟链存在多个中心，由多主体共同运行，〔19〕强调效率与秩序的共存〔20〕。联盟链是在克服传统区块链弊端的基础上发展而成的新形态：其不需要引入算力竞争确定写入权，可以节省计算资源和耗能；其节点数量和区块信息存量较少，有效地提高了数据吞吐能力、系统运行速度，并相应扩展了储存空间；多中心化的特征使其更容易完成特定的任务和目标，有利于提升系统的可控性并实现规范、良性监管。联盟链融合了业务去中心化和管理中心化的双重特点，〔21〕既可以解决信息不对称和隐私保护问题，又便于政府实现特定政策目标。因此，联盟链更适合在由政府主导的场景中应用，是各国政府普遍接受的区块链模式。具体在数字防疫的个人信息治理中，联盟链能够缓解当前数字防疫给个人信息治理带来的风险，且符合我国区块链政策推广和疫情防控的要求。因此，可以利用联盟链缓解数字防疫与个人信息治理之间的冲突龃龉问题。

（一）联盟链可以确保信息真实，创建防控优良信息基础

一方面，联盟链可以激励相关主体提供真实信息。“区块链技术创设的激励机制类似于制度机制，是区块链技术的核心机制之一。”〔22〕联盟链属于“无币区块链”〔23〕，一般不涉及节点争夺记账权问题，但也可根据实际需要设置激励层用来部署激励机制〔24〕。对于个人信息的真实性问题，联盟链可以以积分的方式激励防疫主体上传真实信息并激励有权限的部门积极验证信息的真实性。积分可以用于享有获取信息时的优先权或读取其他地域、部门信息的权限等。链上信息的真实性受到上传和验证的双重激励保证，虚假信息在上传或验证的过程中会被淘汰而不会被记录在系统中，从而保障信息的真实性以创建防控优良信息基础。

另一方面，联盟链可以保证信息真实不被篡改。联盟链具有区块链技术的基本链式结构，能够让链上信息一经储存就无法篡改。〔25〕联盟链系统中的每个区块都包含相连区块的哈希值并相互对应，其中任何一个数值的改变都会导致该区块无法与相邻区块对应，进而不被系统承认。因主观原因上传的虚假信息将永久保存至系统中，无法通过先上传后篡改的方式瞒报、漏报。信息的上传和使用数据同样被记录至系统中。一旦发现不实信息，可以通过系统溯源定位责任主体和使用主体，以尽可能减少损失。对于误记、错记信息的更正和变动，如核酸检测结果变化等，可以通过

〔19〕 参见卜学民：《区块链下证券结算的变革、应用与法律回应》，载《财经法学》2019 年第 3 期。

〔20〕 参见高奇琦：《智能革命与国家治理现代化初探》，载《中国社会科学》2020 年第 7 期。

〔21〕 参见马理、朱硕：《区块链技术在支付结算领域的应用与风险》，载《金融评论》2018 年第 4 期。

〔22〕 胡元聪：《正外部性的经济法激励机制研究》，人民出版社 2021 年版，第 15 页。

〔23〕 邓建鹏：《区块链的规范监管：困境和出路》，载《财经法学》2019 年第 3 期，第 36 页。

〔24〕 参见张楠迪扬：《区块链政务服务：技术赋能与行政权力重构》，载《中国行政管理》2020 年第 1 期。

〔25〕 参见徐琳、袁光：《区块链：大数据时代破解政府治理数字难题之有效工具》，载《上海大学学报（社会科学版）》2020 年第 2 期。

覆盖原有信息以完成，但原有信息不能被删除。此外，“联盟链上的节点采用了实名制的方式”〔26〕，身份相对透明。如果某一节点尝试篡改链上信息，破坏诚信的成本高昂也会使其有所忌惮。

（二）联盟链能够保障信息安全，增强防控信息公信力

一方面，联盟链可以保障信息系统内部安全。优化加密技术是个人信息和隐私保护领域的常用方案。而联盟链的非对称加密技术可以保障联盟链系统内部的信息使用和传输安全。在非对称加密技术的支持下，联盟链上的节点在其权限范围内读写信息。虽然各节点均储存全量账本，但在被系统授权之前，并不意味着该节点自动具备阅读全部账本的权限。这刚好契合防疫部门拥有的信息处理权限差异，即不同节点拥有不同的读写权限。如图 1 所示，可以通过哈希算法将防疫主体 A 上传的个人信息去标识化处理后储存，并借助非对称加密技术对读写权限进行限制，即权限不同的防疫主体对去标识化信息复原程度不同。防疫主体 B 根据其权限对信息复原后使用。这种根据权限非对称加密的有限共享方式，可以有效防控个人信息被泄漏的风险。这就确保了个人信息不会从系统内部泄漏从而增强防控信息公信力。

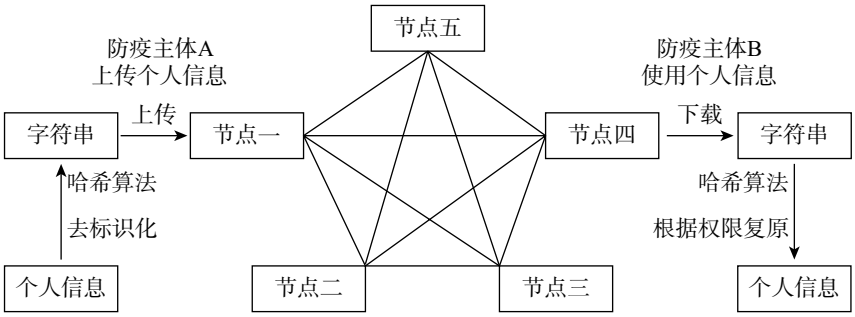

图 1　联盟链去标识化、复原个人信息示意图

另一方面，联盟链可以保证信息系统外部安全。哈希算法可以将储存的个人信息转化为无法破解的 256 位字符串。同时，系统仅保存由算法随机计算得来的字符串，系统外的其他主体无法获得系统内储存的字符串。而系统内的链上节点（即防疫主体）则可以通过匹配私钥和公钥的方式获取个人信息。即使系统因后门漏洞或外部攻击等原因泄露了字符串，也会因为私钥与公钥不匹配、没有签名等原因无法破解其代表的个人信息，不法分子也难以将有限的字符串用于其他用途。此外，联盟链的节点更容易达成新共识，便于进行系统的维护与升级，其算法、协议和加密技术都可以通过中心节点进行更新和审查，相较于其他区块链系统更利于抵抗黑客的外部攻击。〔27〕

（三）联盟链可以促进信息共享，提升防控合作协同效率

一方面，联盟链可以破解信息共享壁垒。联盟链的分布式记账本实质上是一种在节点之间共享、复制和同步的数据库，可以破解信息壁垒，〔28〕进而提高防控合作协同程度及信息治理效率。

〔26〕 翟晨曦、徐伟等：《区块链在我国证券市场的应用与监管研究》，载《金融监管研究》2018 年第 7 期，第 35 页。

〔27〕 参见王延川：《“除魅”区块链：去中心化、新中心化与再中心化》，载《西安交通大学学报（社会科学版）》2020 年第 3 期。

〔28〕 参见胡元聪、谢凤：《智慧司法下数据保护困境突破的区块链技术进路》，载《科技与法律（中英文）》2021 年第 6 期。

通过分布式记账本，防疫主体储存的信息、上传使用记录等储存在系统的每一个节点上。每个节点都是一个信息单元，系统储存的信息在每个单元上记录并共享。只要信息发生变动，就会自动同步记录至所有节点，其他节点则可以根据权限实时读取。同时联盟链只针对特定成员开放，成员需经准入才可参与。这就要求各节点统一信息的上传、储存和传输标准，否则便不能加入系统。这种准入机制一定程度上提高了系统交易性能，可以避免因成员的参差不齐而产生新问题，也在一定程度上缓解了信息不对称问题。〔29〕由此实现链上主体间的信息共享，有效打破“信息孤岛”以提升防控合作协同效率。

另一方面，联盟链可以提高信息共享程度。“代码即信任，是区块链技术的精髓。”〔30〕区块链技术通过算法加持信任以创造良性的去信任化环境，〔31〕利用计算机程序构建新型信任关系，实现点对点交流。联盟链中的节点均通过一定程序获得入链许可和准入，节点所代表的防疫主体资格有一定的保障。且上链信息已经过验证，原本并无合作关系、互不认识的防疫主体之间也无须担心信息的真实性与来源的可靠性，无须经过第三方认证或公证便可直接获取并使用。由此提升了防疫主体的信息共享程度进而提升防控合作效率。此外，可以通过智能合约技术确定信息共享程序，明确防疫主体获取信息的条件以及紧急情况下临时读取信息的处理规则，用代码的方式规范信息共享程序进而提高防控合作协同效率。

联盟链对于化解数字防疫给个人信息治理带来的风险具有天然的优势，在本次数字防疫中也已有相关实践。如广州市南沙区基于“南沙城市大脑”建立了“疫情防控协同系统”，将公安部门、卫生部门、工信部门加入联盟链中。通过联盟链汇总整合了涉疫人员相关个人信息、物资信息等防疫信息，在确保信息真实性、安全性的同时打通了各部门的“信息壁垒”。该系统利用联盟链的不可篡改特征实现企业登记备案的防疫信息不可篡改，保证了信息治理的真实性基础；利用非对称加密机制和哈希算法保障防控重点区域人员涉疫信息安全，提升了防控信息公信力；利用分布式记账本等实现区域内各部门的相关信息实时共享，提高了信息治理效率；利用智能合约技术为相关企业疫情防控承诺提高可信度。“南沙疫情防控协同系统”利用联盟链构建了传播过程不可逆、可有效溯源追踪且有约束力的信息治理系统，为数字防疫中个人信息的治理联盟链的应用提供了一定的经验。

四、数字防疫中“链”“法”协同机制的理论基础

联盟链因其特殊的技术架构对于化解数字防疫给个人信息治理带来的风险具有积极作用，但联盟链的技术特征与传统法律模式也存在天然的矛盾。联盟链虽然经过多中心化改造，对于政府实现特定政策目标和监管具有积极意义，但联盟链毕竟采用了区块链技术的基本架构，其应用将导致传统技术逻辑和业务逻辑发生较大变化，使传统法律法规的适用产生新问题。因此，应当妥善处理二者之间的关系。下面将对区块链技术与法律，即“链”“法”的关系模式进行分析，以

〔29〕 参见张礼卿、吴桐：《区块链在金融领域的应用：理论依据、现实困境与破解策略》，载《改革》2019 年第 12 期。
〔30〕 任仲平：《区块链领导干部读本》，人民日报出版社 2018 年版，第 10 页。
〔31〕 参见赵增奎：《以区块链技术推动互联网金融稳健发展研究》，载《经济纵横》2017 年第 11 期。

求得在数字防疫的个人信息治理中，联盟链与法律之间的最优“相处模式”，通过消除联盟链和法律之间的张力，使二者相互“磨合”，构建“链”“法”协同机制以提升其在数字防疫中个人信息治理方面的能力。

（一）“链”“法”的关系模式类型及评析

1.“链”“法”的关系模式类型

自科技革命以来，如何协调法律与新兴技术之间的关系成为人类社会发展面临的重要议题。新兴技术在基因改造、生物克隆、自动驾驶、信息交流等方面带来了空前的福利，也对现有法律产生了严峻的挑战。“技术一旦进入社会领域，必然会被社会制度、社会组织和社会群体的各种利益、诉求和价值判断所塑造和限制。”〔32〕目前，“链”“法”之间的关系主要有三种类型：管制模式、替代模式和互补模式。管制模式表现为国家通过法律对区块链技术进行严格管制，其坚持较为传统与保守的理念。如果区块链技术可以实现特定社会目标，就通过法律对区块链技术进行保护和激励；如果区块链技术不能实现目标，就要通过法律进行压制。〔33〕源于金融危机等历史原因，一些国家对虚拟货币和区块链技术采取非常谨慎的态度，因为担心技术创新和应用会对社会产生负面影响，所以对区块链技术进行严格管制。替代模式与管制模式截然相反，其是处理“链”“法”关系的前卫观点，认为区块链技术可以完全替代法律，即“政府可以利用区块链技术建立自己的规则系统，通过自动执行的代码系统以带来规则执行效果和效率的革命性提升”〔34〕。这种“代码即法律”的观点在国外已有诸多探讨。与前两种模式不同，互补模式介于管制模式和替代模式之间，其认为“链”“法”各有优势，应当发挥二者各自优势从而构建“链”“法”的共同应用模式。即应当在现有法律制度较为完备的情况下，应将区块链技术作为技术手段，补充现有法律以提高效率并降低交易成本。如“区块链＋发票”，通过应用区块链技术加强税收征管，促进了税收管理制度的完善。

2.“链”“法”的关系模式评析

管制模式和替代模式都是“链”“法”“分立”并相互“对抗”的结果。在管制模式中，法律占据了上风：面对区块链技术应用带来的挑战，法律拒绝做出大的调整，其强势要求区块链技术为符合社会利益而调整。这种模式可以最大程度上防范风险，对区块链技术应用暴露的安全性问题可以及时制止，但是其也会导致诸多负面影响：一方面简单将法律作为压制技术的工具，既否定了法律独特的治理价值，也破坏了法律实践的自主性及法律自身所具有的教义学结构；另一方面也否定了区块链技术的社会建构价值，最终破坏区块链技术的社会效用。在替代模式中，区块链技术获得了胜利：法律顺应区块链技术的价值进行自我调整和革新。但用区块链技术和代码完全替代法律未免过于极端。区块链技术是近年出现的新型信息技术，在智能合约、自动执行等方面迅猛发展。其作为一种去中心化的、安全的、难以破坏的数据簿，虽有自身的价值，但也有固

〔32〕 郑玉双：《破解技术中立难题——法律与科技之关系的法理学再思》，载《华东政法大学学报》2018 年第 1 期，第 87 页。

〔33〕 参见赵小勇：《法律与技术如何相处：区块链时代犯罪治理模式的双重重构》，载《探索与争鸣》2020 年第 9 期。

〔34〕〔法〕普里马韦拉·德·菲利皮、〔美〕亚伦·赖特：《监管区块链——代码之治》，卫东亮译，中信出版集团 2019 年版，第 211 页。

有的缺陷。用代码完全取代法律规则并不可行，也不合常理。法律作为带有国家意志的强制性社会规范，有其自身的优势并可持续修改完善，仍将长期作为规制社会信任的规则。在互补模式中，区块链技术与法律非但不会相互“对抗”，还可能“携手共进”，呈现相辅相成的关系。易言之，法律展现了对区块链技术的宽容，在现有法律框架内对区块链技术的应用进行回应。事实上，法律和区块链技术各有优势，区块链技术可以利用代码更好地实现事前预防和事中规范，法律凭借其强制力、规范性等可以实施有力的事后追责救济和监管。总之，区块链技术和法律各具优势，可以取长补短，通过区块链技术的应用补充和保障法律的实施。

（二）“链”“法”协同机制的选择原因及思路构想

1.“链”“法”协同机制的选择原因

联盟链对于化解数字防疫给个人信息治理带来的风险具有独特的优势，但是联盟链并不能完全替代法律，因为联盟链同样具有区块链技术自身的局限性。联盟链虽然经过多中心化改造，但同样具备分布式记账本的特征，其诞生之初就可能带有除实现特定目标之外的其他主观目的。〔35〕同时，“代码并不比制度更中立，其也受制于垄断和商业利益”〔36〕。此外，区块链技术虽然建立了特殊的信任系统，但信任系统并非完美无缺：其以现代密码技术为基础，仍存在被攻破的可能性；系统的安全和稳定还在不断地发展和变化之中，选择最优的运营模式还需一定时间；智能合约和其他软件代码一样也存在误差和安全漏洞，加之系统直接运作信息价值或财产权利，智能合约误差和漏洞的存在就显得极其危险；现有智能合约技术距离支撑法律的自动执行还有一定的差距。〔37〕因此，存在的悖论是：区块链技术为降低风险而应用，但区块链技术的应用带来了新的风险，其应用带来的外部性问题仍需要法律进行解决。

在数字防疫中，联盟链也无法全部取代法律在个人信息治理方面的作用。法律规范由人类语言构成，具有灵活性和模糊性，“具备通过不断的调试和进化来妥善处理新生事物的能力”〔38〕，可以适应立法者立法时不能预见到的各种偶然性。联盟链由代码语言构成，具有机械性和确定性，只能适用于可以客观验证并已经在底层代码中预先定义的规则。将人类语言构成的开放式法律转化为代码，容易产生歪曲法律含义的风险。这里存在的悖论是：虽然区块链技术是面向未来的技术，但其也无法适应编写时不可预见的未来。由于代码语言的确定性，用严格和正式语言编写的技术治理规则通常无法适用于处于法律灰色地带的意外案件，也很难提前充分考虑并在基础代码中写入即将出现的所有可能性。在出现更先进的“强人工智能系统”之前，代码对于数字防疫中个人信息治理方面可能出现的不可预见情况缺乏适应和解释能力。此外，法律可以通过强制力处罚公民财产、限制人身自由甚至剥夺公民生命，且有一定程度的纠错可能，而代码却无法承担如此重负：一旦代码误判、错判，当事人就会面临人身和财产被代码自动执行而受到严重侵害并无法纠错的巨大风险。因此，技术的迭代并不能完全代替制度的作用，联盟链也不能完全代替

〔35〕 参见赵蕾、曹建峰：《从“代码即法律”到“法律即代码”——以区块链作为一种互联网监管技术为切入点》，载《科技与法律》2018 年第 5 期。

〔36〕〔英〕罗伯特·赫里安：《批判区块链》，王延川、郭明龙译，上海人民出版社 2019 年版，第 32 页。

〔37〕 参见〔美〕凯文·沃巴赫：《链之以法——区块链值得信任吗?》，林少伟译，上海人民出版社 2019 年版，第 47 页。

〔38〕 殷秋实：《智能汽车的侵权法问题与应对》，载《法律科学（西北政法大学学报）》2018 年第 5 期，第 48 页。

法律。在应用联盟链治理风险的同时还需要对相应制度进行优化，从而在技术迭代与制度优化的作用下实现联盟链与法律的“携手共治”。基于此，我们认为，“技制共治”开辟了提升国家治理能力的新路径。

2.“链”“法”协同机制的思路构想

在数字防疫的个人信息治理中，可以采用互补模式，融合“链”“法”的优势构建协同治理机制。“如果现有法律信任结构仍可以普遍适用，按照现有的法律规则能够进行一定程度上的规制，那么区块链技术应该成为法律的补充和保障，其主要价值在于提升信息记录的效率和安全。”〔39〕管制模式和替代模式都有其不足，二者代表的区块链技术与法律分立的观点会带来各种弊端并增加区块链技术创新和传统法律之间的冲突龃龉问题。此外，联盟链和法律在数字防疫的个人信息治理中均有规范、保护个人信息的功能，只是实施方式和手段有所不同。联盟链通过技术手段，利用代码建立自动执行模式，规范个人信息的储存、利用程序，从技术角度实现对个人信息的技术治理。而法律通过制度手段，利用强制力规范各方权利、义务和责任，从制度角度实现对个人信息的法律治理。技术治理与法律治理尽管在治理逻辑上存在差异，但二者也存在巨大的互补性。正确处理技术治理与法律治理的关系，形成共治结构，是提升我国治理水平和能力的前提。〔40〕基于此，可以采用“链”“法”的互补模式。在数字防疫中，可以利用联盟链和法律各自的优势，采取联盟链和法律协同作用的个人信息综合治理模式，构建以法律为主体、以联盟链为辅助的“链”“法”协同治理机制。

具体而言，在“链”“法”协同治理机制中，联盟链和法律的分工有所不同。一方面，法律是数字防疫中个人信息治理的基础和前提。法律在此主要起到明确联盟链的法律地位和效力、实现追责救济、实现全程动态监管的作用。首先，法律可以明确联盟链在数字防疫中个人信息治理方面的法律地位和效力。法律具有普遍性的特征，可以根据数字技术的特征、个人信息的治理需求及疫情防控形势，明确联盟链的法律地位以及分布式记账本、智能合约等技术的法律效力，做到有法可依。其次，法律可以实现事后的追责与救济。法律具有国家强制力的特点，可以配合联盟链的溯源机制确定相关案件的事实问题，对相关案件起到定分止争的作用，对责任主体和损害主体进行强有力的追责和救济。最后，法律可以实现全程动态监管。法律具有规范性的特点，可以配合联盟链的多中心化特征进行实时监管，转变原有事前准入、事后监督的传统监管模式为实时发现风险、及时处理并加以预防的全程动态监管模式。

另一方面，联盟链是数字防疫中个人信息治理的保障和补充。联盟链在此主要起到降低个人信息治理风险、帮助法律进行追责和监管、一定程度上替代规则的作用。首先，联盟链可以降低数字技术对个人信息治理产生的风险。如前文所述，面对数字技术对个人信息治理可能产生的风险，联盟链可以提升个人信息治理的真实性以创建优良信息基础，能够保障个人信息的安全性以提升信息公信力，可以促进个人信息的共享程度以提升协同效率。其次，联盟链可以助力法律进行追责和监管。联盟链作为一种技术解决方案，有其自身的优势，从而帮助法律提升实施效果。

〔39〕〔美〕凯文·沃巴赫、林少伟：《信任，但需要验证：论区块链为何需要法律》，载《东方法学》2018年第4期，第107页。

〔40〕参见郑智航：《网络社会法律治理与技术治理的二元共治》，载《中国法学》2018年第2期。

如联盟链多中心化的特征可以帮助法律进行监管从而实现疫情的精准防控。再如数字时代个人信息保护的重点应当由传统的事前保护转移到事中、事后的保护,〔41〕而联盟链可以配合法律在数字防疫中规范个人信息的事前收集、事中处理的程序,以及在事后救济的取证方面提供助力。最后,联盟链可以实现一定程度上代替规则自动运行的作用。利用代码创设的自动化应用程序可以在一定程度上代替相关制度规则。如监管部门可以利用代码在监管节点创设自动执行的监管程序。当系统达到特定要求即可能产生风险时,自动发出警示以要求相关节点说明情况,甚至暂缓传输信息,以此代替原有规范性文件规定的相关程序性风险防范规则。

五、数字防疫中“链”“法”协同机制的构建思路

(一)构建与法律相匹配的联盟链治理机制

如前所述,联盟链是数字防疫中个人信息治理的保障和补充。在“链”“法”协同治理机制中,首先需要构建与法律相匹配的个人信息联盟链治理机制,即建立个人信息联盟链治理系统。这一过程既要动态认识联盟链的优势与法律的相对劣势,也要考虑我国数字防疫的现实,具体可以从以下三个方面展开:

1. 制定联盟链底层技术标准

联盟链作为新兴技术,其在数字防疫中的应用应当首先明确其使用的底层技术标准。建设数字防疫中个人信息治理的联盟链系统将是一个复杂的系统性工程,“链”与“非链”信息系统将长期共存。如果不能采用统一的信息格式和标准,则“容易引发系统错误、混乱等风险”〔42〕,也无法实现不同信息系统之间的信息互通。信息只能在联盟链系统内流通,使联盟链系统成为更大的“信息孤岛”,即“区块链孤岛”〔43〕,从而不能实现本质上的信息共享。制定统一的联盟链底层技术标准,可以彻底打破“信息孤岛”现象,使个人信息在“链”与“非链”中有序共享,从而提升信息治理效率;也可以为联盟链在其他领域的应用提供标准和参考,从而推动区块链产业协同发展。当前区块链产业仍处于发展初期,存在一定程度的行业乱象,各区块链服务商的技术水平和研发能力均有待加强。制定统一的联盟链底层技术标准,可以为区块链技术服务商提供标准指导,从而推进防疫主体控制的个人信息持续上链存储;也可以为数字防疫中的个人信息治理提供相关决策和监督尺度参考,从而提升监管能力和安全保障水平。本文建议:应当由防疫主管部门和工信部门负责,会同科研机构、专家学者立足现有联盟链成果,参考现有技术规范,制定数字防疫中个人信息治理联盟链系统底层技术标准,明确数据接口、共识机制、分布式记账、智能合约等代码标准和加密程度、算力空间、登录 IP 地址限制等运行规则;应当围绕数字防疫的紧迫性、个人信息的安全性需求和联盟链的优势提出此联盟链系统的底层技术要求,明确该系统的建设及运行标准;确保数字防疫中个人信息治理联盟链系统规范建立并良性运行,保证其和其他“链”与“非链”信息系统协同发展。

〔41〕 参见邢会强:《大数据时代个人金融信息的保护与利用》,载《东方法学》2021 年第 1 期。

〔42〕 杨东:《链金有法——区块链商业实践与法律指南》,北京航空航天大学出版社 2017 年版,第 309 页。

〔43〕 胡元聪:《区块链技术激励机制的制度价值考察》,载《现代法学》2021 年第 2 期,第 153 页。

2. 构建联盟链应用平台框架

联盟链对于化解数字防疫给个人信息治理带来的风险具有天然的优势，其多中心化的特征也有利于政府统一管理，从而实现精准防控。可以利用联盟链搭建数字防疫中个人信息治理的应用平台框架，建立包括监管部门、防疫主体（包括公权力防疫部门和社会防疫主体）在内的多中心联盟链系统。疫情防控需要社会各界共同参与，在国家的统一管理下实现联防联控。因此，新系统既要强化国家的中心管理作用，也要注重各行各业的参与。〔44〕在联盟链治理系统中，应当由各级政府和监管部门成为中心节点，强化国家的中心管理作用；并采用政府主导、法律政策推动的形式，将数字防疫中涉及的其他公权力防疫部门、相关社会防疫主体作为普通节点纳入系统中，使涉及疫情防控和个人信息治理的部门、企业一起联防联控，形成“共治”〔45〕机制。并根据数字防疫和个人信息治理的特点，在系统存储总量、响应速度等方面优化改进。对此，可以通过规范性文件明确各级政府和监管部门的中心节点资格，并明确其他公权力防疫部门、相关社会防疫主体的普通节点资格，并排除其他主体的节点资格。此外，可以在系统中设立没有写入权限的访问节点，供其他没有成为系统节点的主体获取信息。在数字防疫中，自然人作为信息的被处理者具有随机性，而个别社会防疫主体如社区、村委会等不容易满足加入联盟链的设备条件和制度要求，因而这些主体不被纳入联盟链系统中。但是，可以通过联盟链上没有写入权限的统一访问节点，使自然人访问其在系统中储存的本人和亲属的个人信息供其他防疫主体校验，从而使社区、村委会等个别没有成为节点的社会防疫主体也可以通过联盟链获取其权限范围内的相关防疫信息，由此在保障联盟链技术性能的前提下提升联盟链的覆盖范围，使更多主体分享技术迭代带来的“红利”。

3. 建立联盟链技术处理规则

具有规范、安全的技术处理规则是联盟链系统有序运行的前提。在联盟链系统的建设及运行过程中，应当依托现有地方联盟链防疫系统，建立信息上传、利用的技术处理规则，保证数字防疫中个人信息的安全利用。

首先，应当建立信息上传的技术处理规则，结合实践分批上传个人信息。数字防疫中涉及的个人信息数量众多，信息入链的先后顺序需要得到规范。因此，应当建立信息上传的技术处理规则，结合当前我国疫情防控实际和联盟链发展现实，根据地域分批建立联盟链系统，依据涉疫程度分批上传个人信息：其一是依托现有济南、广州等地的联盟链防疫系统优先上传济南、广州等联盟链防疫实践地区的疫苗接种者、确诊、疑似、无症状患者及密切接触者的个人信息；其二是上传当前及近期中、高风险地区的疫苗接种者、确诊、疑似、无症状患者及密切接触者的个人信息；其三是上传当前及近期中、高风险地区其他人员、境外入境人员、高危感染人员的个人信息；其四是进行疫苗接种者、曾经确诊、疑似及无症状感染者的个人信息上传；其五是进行全国范围内的普遍上传。

其次，应当建立信息利用的技术处理规则，按照分层分级储存、根据权限下载的原则利用个

〔44〕 参见黄茂汉：《基于区块链技术的疫情防控情报系统模型研究》，载《情报科学》2021 年第 8 期。

〔45〕 杨杨、杜剑等：《区块链技术对税收征纳双方的影响探析》，载《税务研究》2019 年第 2 期，第 116 页。

人信息。数字防疫中涉及的信息处理主体众多，个人信息的利用程序需要得到规范。因此，应当建立信息利用的技术处理规则，将节点搜集到的个人信息根据不同属性和来源利用非对称加密技术分级、分层储存，并依照防疫部门的权限确定其访问和使用的边界。个人信息在节点去标识化上链储存后，分为不同保密级别的信息。保密级别较低的信息主要包括去标识化的身份信息、活动轨迹等基础信息，对防疫主体的访问权限限制较低。保密级别较高的信息主要包括实名身份信息、接触史等个人涉疫信息，只允许具有较高权限的防疫主体访问。应当通过联盟链的共识机制和非对称加密机制设立差异化的信息访问权限，以此保证个人信息安全。

（二）构建与联盟链相适应的法律治理机制

法律是数字防疫中个人信息治理的前提和基础。在“链”“法”协同治理机制中，需要构建与联盟链相适应的数字防疫个人信息法律治理机制。法律应当改变传统的治理模式，适应联盟链环境并与之共同构建全方位的协同治理机制。具体可以从以下三个方面展开：

1. 明确联盟链的法律地位和效力

推动联盟链在数字防疫中个人信息治理方面的应用，应当考虑相关技术应用的法律基础，明确联盟链的法律地位和法律效力是“链”“法”协同作用的前提。首先，应当明确联盟链的法律地位。目前，我国个人信息治理的法律规则规定于由《民法典》和《个人信息保护法》组成的个人信息保护制度体系中，但其未对重大突发公共卫生事件背景下个人信息的治理和智能技术的应用给予明确规定，而仅为一些纲领性的总括，导致这一特殊背景下智能技术在个人信息应用方面的相关法律规范仍分散于诸多法律文本中。而联盟链对个人信息治理具有重大促进作用，将从技术手段破解原有信息治理难题。对此，应当肯定联盟链作为治理手段和治理工具的法律地位，并制定相关激励条款，肯定并鼓励联盟链在个人信息治理方面的应用，促进联盟链乃至智能技术在个人信息治理方面相关产业的发展。其次，应当明确联盟链的法律效力。目前，联盟链已经在司法层面初步得到肯定。最高人民法院在《关于互联网法院审理案件若干问题的规定》中对于利用哈希值校验、区块链技术搜集的证据予以认可，部分司法裁判中也已肯定利用区块链技术存证的法律效力。〔46〕但如果想让联盟链在数字防疫和个人信息治理中更好地发挥作用，需要给予更高层面的确认。联盟链可以成为法律的补充，和法律协同化解数字防疫给个人信息治理带来的风险。因此，应当出台相关法规或调整相应规范，对联盟链的分布式记账本的信息记录、智能合约等有效性进行确认，肯定联盟链在个人信息治理方面的法律效力。

2. 构建适合联盟链的节点责任制度

构建基于联盟链的节点责任制度是法律适应联盟链分布式分类账环境的重要转变。联盟链的分布式记账使得系统内并不存在传统平台上的唯一中心化管理主体，原中心化职能被分散给相关多个中心节点。故在“链”“法”协同机制中，为适应联盟链这一特征，可以立足于系统节点，建立适应联盟链的节点责任制度。

首先，应当通过法律明确节点为责任主体。节点对于分布式记账本具有重要意义，是整个联盟链系统的参与主体，系统通过节点之间的相互验证、记录得以运转。联盟链的节点身份固定且

〔46〕 参见吴京辉、胡兰：《区块链技术助推中小企业票据融资的法律完善》，载《江西社会科学》2019 年第 12 期。

透明，由防疫部门、监管部门组成，可以准确定位节点对应的防控主体，并不存在其他区块链系统因节点匿名而无法追责的问题。根据本次防控实践，个人信息可能部分泄漏于防疫机关。因此，应当明确联盟链系统节点的责任主体资格，即节点应当作为承担责任的主体。其次，应当明确系统节点的责任内容。我国对区块链系统节点的义务与责任已有初步规定。国家网信办《区块链信息服务管理规定》规定了提供区块链信息服务的主体或节点的管理、配合监管等义务及相关的责任，但该文本中的规定较为粗糙，更多的是一些纲领性的宣誓条款，其中一些概念的具体含义并不明确。〔47〕因此，应当对该部门规章进行修改，或就该文本展开进一步的解释与探讨。在数字防疫中，应当明确防疫主体在原信息处理相关义务外，作为联盟链系统节点而具有的权利、义务和责任，并明确其责任形式及追责程序。通过追责弥补联盟链“技治”无法涵盖的部分漏洞和不足，如联盟链可以通过激励机制保证链上信息的真实性，但对于上传前信息的真实性无法保证，对此可以发挥法律的约束功能，明确上传虚假信息的责任和相关过错或知情方的责任以弥补联盟链的不足，实现联盟链的技术激励与法律的制度约束的协同。同时，对于节点责任的形式应当注重民事、刑事和行政责任的并用，在对违反义务的行为加大行政处罚力度的同时辅以民事赔偿责任。此外，还要明确节点代表主体责任人的责任并落实到人，对于达到刑事责任标准的行为加以刑法的规制以发挥刑法的震慑作用。

3. 建立适应联盟链的动态监管制度

建立基于联盟链系统的动态监管制度可以助推法律由事前准入、事后监督的传统监管模式转向全程动态监管模式以适应联盟链系统。联盟链的加密机制、链式结构等将联盟链系统分隔为链上链下两个世界，链上的空间运行状态公开透明，每个节点都在参与系统的运行，而基于联盟链的多中心化特征也适合嵌入若干监管节点。故在“链”“法”协同机制中，可以构建基于联盟链系统的全程动态监管模式，将部分中心节点设为监管节点并使监管部门加入其中。如此不仅能够借助联盟链实现实时监管，还可以监测并预防联盟链应用可能带来的未知风险。首先，应当成立超级监管节点。在系统中将部分中心节点改造为监管节点，监听链上广播、储存信息，更新全网总账，掌握系统动态。一方面，监管部门通过监管节点实时获取系统内的共享信息，掌握链上活动，可以及时发现违法违规现象，提高监管效率。另一方面，监管部门通过监管节点实现一定程度上的自动执行和实时决策，可以及时根据系统运行情况变动系统规则进而有效预防可能发生的风险。其次，应当成立公权力监管部门，并通过法规或部门规章赋予其超级监管节点资格。即明确将数字防疫中个人信息治理监管权交由国家统一调度，由国务院主导，工信部会同网信办负责，协调多方职能部门，设立中央和地方层面的数字防疫中个人信息治理联盟链系统监督管理委员会。该委员会统筹领导联盟链系统的推进及监管工作，并作为超级节点被加入系统中，对系统进行实时监测。〔48〕同时明确该监管部门在事前审查、事中管理以及事后追责等阶段使用的程序和对应职责。还要赋予该监管部门独立的执法权和管理权，避免部门之间互相推诿等情况，促进数字防疫中个人信息治理联盟链系统监管规范化。最后，应当设立社会层面的行业协会。有必要

〔47〕参见贾翱：《区块链信息服务监管对象研究——以〈区块链信息服务管理规定〉第二条为中心》，载《大连理工大学学报（社会科学版）》2020 年第 2 期。

〔48〕参见时明生：《区块链技术在征信业的应用探析》，载《征信》2018 年第 1 期。

在监管部门之外设立独立的行业协会，并给予其一定自主权限。该协会可以针对联盟链系统发展的形势制定行业自律标准和实施细则，对系统进行定期风险评估与调查监测，同时促进信息持续上链和系统平稳运营以减轻公权力机关负担。

六、结　语

联盟链对于化解数字防疫的个人信息治理风险具有天然优势，可望缓解数字防疫与个人信息传统法律治理之间的冲突龃龉问题，进而破解个人信息治理之“危”，利用数字进行防疫之“机”。但基于联盟链的“技治”并不能完全取代基于法律的“制治”，以代码替代法律的设想也不可行。应当发挥联盟链的长处，结合法律治理的优势来构建数字防疫中个人信息“链”“法”协同治理机制。在大数据、人工智能等技术基础上继续应用联盟链是一项系统工程，应当在不断实践的基础上充分把握联盟链、法律各自的优势，以及数字防疫和个人信息治理的发展趋势，缓解联盟链与法律、数字防疫与个人信息治理之间的双重张力。同时需要指出：以联盟链为代表的区块链技术毕竟属于新兴技术，在应用方面仍处于探索阶段。联盟链应用可能带来的风险和挑战还需要进一步的探讨。

Abstract：In this epidemic prevention and control，digital technologies such as artificial intelligence and big data not only reduce the risk of epidemic spread，but also make personal information management face new risks. Alliance chain has been widely used in many fields in recent years，and has become a feasible tool to resolve the risk of personal information governance in digital epidemic prevention. However，while applying alliance chain governance risk，it is also necessary to optimize the corresponding system，so as to realize the “joint governance” of alliance chain and law under the action of technical iteration and system optimization. Therefore，we should eliminate the tension between alliance chain and law，and then build a “chain” and “law” coordination mechanism based on legal governance and supplemented by alliance chain governance. Specifically，by building an alliance chain governance mechanism matching the law and a legal governance mechanism matching the alliance chain，and integrating the respective advantages of blockchain technology and law，the “chain” and “law” coordination mechanism can improve its ability in personal information governance in digital epidemic prevention，thus improve the level of modernization of national governance.

Key Words：digital epidemic prevention，personal information governance，risk government，alliance blockchain，synergy between “blockchain” and “law”

（责任编辑：殷秋实　赵建蕊）

财经法学 No. 3，2022
pp. 65 - 79

“国家在场”视角下个人信息保护的实践检视与路径探索

王　娅*

内容提要：个人信息的保护与利用牵涉个人、企业和政府之间的利益与权力关系。国家需要作为独立的行为主体，调和参与者之间的冲突，整合个人信息保护实践。维护个人的知情同意规则、约束企业的隐私政策以及要求政府的行政规制这三种实践表明：在个人信息保护领域，国家在场是一个既成事实。然而，国家在场的实践存在两方面问题：一是内容上全面兼顾了个人权利、企业责任与政府义务，但各主体的履行实效欠佳，难以切实维护个人的合法权益；二是形式上以规范信息处理者的活动为主，但规制策略的取向不明，难以恰当界定企业自我规制与政府规制之间的关系。因此，信息时代国家的有效在场，需要重申人性尊严的基本理念，以维护个人的主体地位，也需要重述规制策略的主要共识，确立回应型规制，以妥善对待企业与政府之间的互动。

关键词：国家在场　个人信息保护　知情同意　企业自我规制　政府规制

一、问题的提出

全球个人信息保护立法的实践，如欧盟《通用数据保护条例》、美国《隐私权法》以及我国《个人信息保护法》，呈现出很强的国家引领和布局的色彩。个人信息保护立法的本质是国家对个人信息处理行使规制权。〔1〕个人信息保护是国家事务的组成部分，也是国家治理的重要场域，深受国家影响与支配。国家自始至终伴随着个人信息的书写、解释和演进，与个人信息保护紧密相

* 王娅，吉林大学法学院博士研究生。

本文为国家社科基金重大专项项目“核心价值观融入法治建设研究：以公正司法为核心的考察”（17VHJ007）、教育部人文社会科学研究专项项目“新时代中国特色社会主义法治思想研究”（18JF210）的阶段性成果。

〔1〕 See Colin Bennett，Charles Rabb，*The Governance of Privacy：Policy Instruments in Global Perspective*，Ashgate，2003，p. 95.

连并持续互动，国家的显现也是个人信息能被持续保护的重要动因。因此，在个人信息保护领域，国家以何种方式在场，产生了什么影响以及未来努力的方向何在，是必须予以清晰回答的重要问题。对这些问题的有效回答，一方面有助于提高国内整体的个人信息保护水平，另一方面也有助于增进国际社会对中国个人信息保护制度的认可，为后续推进跨境数据流通机制创造积极条件。

既有的学术探讨主要围绕个人信息保护的权益基础、〔2〕归属的法益领域、〔3〕实践中的价值取向、〔4〕理论导向，〔5〕以及未来的路径选择〔6〕等方面展开。这些研究虽贡献了诸多智识，但大都以个人信息为关注点，过滤了对个人信息保护进行宏观全面认识的可能。进而言之，既有研究多从“如何保护”这一内部路径探寻着手，忽略了“国家如何主导参与者的互动实践”这一外部视角的观察与省思，这导致既难以对参与者之间的互动与博弈进行细致观察，又难以精准把握未来个人信息保护的方向与行动。因此，有必要爬梳国家在个人信息保护中的表现形式及其影响，并探索如何更好地将《个人信息保护法》中的国家意志具体化，以实现宏观议题的微观切换。

本文拟采用“国家在场”视角审视个人、企业与政府〔7〕之间的具体互动与典型实践，阐明国家对个人信息保护实践的影响，并在此基础上探讨个人信息保护的未来方向与行动要旨。

二、个人信息保护领域“国家在场”视角的引入

“国家在场”视角被广泛用于解释我国的经济、社会、法律与文化等领域的诸多现象和问题，取得了丰硕成果。然而，学者们对此概念的内涵尚未形成完整明确的界定。因此，在考察“国家

〔2〕 例如，欧盟有人格权保护模式，美国有隐私权保护模式。也有人称之为“数据保护法模式”和“消费者保护模式”。两者之间的主要区别在于默认规则，前者仅在法定理由之下才允许收集和处理数据；后者则相反，一般允许收集和处理个人信息，除非特别禁止。See William McGeveran, Friending the Privacy Regulators, 58 *Arizona Law Review*, 966 (2016).

〔3〕 主要有公法保护模式、私法保护模式和综合保护模式之争。参见赵宏：《〈民法典〉时代个人信息权的国家保护义务》，载《经贸法律评论》2021 年第 1 期；宋亚辉：《个人信息的私法保护模式研究——〈民法总则〉第 111 条的解释论》，载《比较法研究》2019 年第 2 期；程关松：《个人信息保护的中国权利话语》，载《法学家》2019 年第 5 期。

〔4〕 有过程保护与结果保护的分野，也有分享优先与控制优先的选择。参见蔡培如：《个人信息保护原理之辨：过程保护和结果保护》，载《行政法学研究》2021 年第 5 期；陆青：《数字时代的身份构建及其法律保障：以个人信息保护为中心的思考》，载《法学研究》2021 年第 5 期；杨贝：《个人信息保护进路的伦理审视》，载《法商研究》2021 年第 6 期。

〔5〕 主要有个人信息自决论、社会控制论和国家保护义务论的理念反思。参见高富平：《个人信息保护：从个人控制到社会控制》，载《法学研究》2018 年第 3 期；王锡锌：《个人信息国家保护义务及展开》，载《中国法学》2021 年第 1 期。

〔6〕 主要有法律保护、技术设计与伦理审视等多种进路。参见郑志峰：《通过设计的个人信息保护》，载《华东政法大学学报》2018 年第 6 期；肖成俊、许玉镇：《大数据时代个人信息泄露及其多中心治理》，载《内蒙古社会科学（汉文版）》2017 年第 2 期；前引〔4〕，杨贝文。

〔7〕 政府是国家意志的合法代理者，“国家”与“政府”往往相互替用。但本文将国家定位为超然的、中立的角色，用以居中调和个人、企业和政府之间的权益冲突。一方面是因为国家本身可以如西达·斯考切波（Theda Skocpol）所期望的那样，作为独立的“行为体”参与并追求某些社会目标；另一方面，政府兼具利用者与监管者的双重身份，始终难以对这两类身份保持反思性隔离，甚至在实践中很可能不经意地以双重身份相互解释或者错位使用。因此，把政府置于国家视角之下去思考，某种程度上避免了这种尴尬境地。再者，《个人信息保护法》中也将“国家”“处理个人信息的国家机关”“履行个人信息保护职责的部门”三者之间进行了称谓和职能上的区分，比如“国家”出现了 2 次，用以表明国家在个人信息保护方面的态度和行为，即建立健全个人信息保护制度以及积极参与个人信息保护国际规则的制定。See Peter B. Evans, Dietrich Rueschemeyer, Theda Skocpol, *Bringing the State Back in*, Cambridge University Press, 1985, p. 9.

在场”视角下个人信息保护实践之前，有必要对“国家在场”的学术意涵做进一步限定。从结构上考察，“国家在场”具备实体论与方法论两个维度。就实体内容而言，“国家在场”是重要的理论模式，表达的是国家及其公权力对传统公共领域乃至私权领域的渗透。〔8〕作为一种重要的方法论，“国家在场”有助于对复杂的社会关系网络和多样的社会生产结构做出二元化透视，便于揭示隐匿于人类生活中的社会规律。〔9〕学者们使用“国家在场”，多是基于方法论层面，将其作为一种分析框架实现对社会现象的合理认知。

（一）“国家在场”的学术意涵与理论脉络

“国家在场”最早出自美国学者乔尔·米格代尔（Joel S. Migdal），意指一种“国家在社会中”的研究视角（a state in society perspective），〔10〕被用来检视国家和社会之间分组整合及其合纵连横的互动过程。20世纪90年代初，我国学者高丙中较早使用这一方法并引起广泛关注。他把米格代尔的“国家在社会中”直译为“国家在场”，即“以国家的视角来研究社会问题，进而对既往社会研究中所普遍存在着的内生主义倾向进行纠偏”〔11〕。此后，这一分析框架不断扩充，先后渗透到民族学、政治学、社会学等相关领域，为重新认识国家与社会的关系提供了一种新的解释模式。〔12〕但是，已有的研究并没有明确界定这一概念，只是用来描述国家对社会的影响以及社会对国家的回应之现象。

除了上述整体性理解之外，“国家在场”的概念还存在“国家＋在场”的组合式理解。作为概念组合的“国家在场”，其重点在于对“场（域）”的理解。“场域”概念的使用源于布尔迪厄（Pierre Bourdieu）。受黑格尔影响，他在“场域”的思考中加入“现实的关系”之因素。其后，他受马克思启发，给“场域”的思考注入“客观存在”的因素。因此，在布尔迪厄看来，场域是“在各种位置之间存在的客观关系的一个网络或一个构型（configuration）”〔13〕。他认为，当场与权力结合起来时，国家就是一个不可规避的权力结构，且与其他社会力量相结合，表现为一种多维度、多向度的运行。〔14〕因此，“国家在场”即是以国家的力量影响、作用或控制各种社会关系。

〔8〕参见王建生：《西方国家与社会关系理论流变》，载《河南大学学报（社会科学版）》2010年第6期；邓正来：《国家与社会：中国市民社会研究》，中国法制出版社2018年版，第16－18页。

〔9〕参见廉睿、高鹏怀：《“国家在场”与族群法治知识功能再造——基于西北T自治县生态保护的田野调查》，载《广西民族研究》2018年第4期。

〔10〕20世纪80年代，以彼得·埃文斯（Peter Evans）为代表的学者仅关注国家自主权和国家能力等方面的研究，这被称为国家中心主义。但国家中心主义很快受到挑战，以米格代尔为代表的学者坚持社会中心主义的立场，以回应国家中心主义的研究。参见〔美〕乔尔·米格代尔等编：《国家权力与社会势力：第三世界的统治与变革》，郭为桂等译，江苏人民出版社2017年版，第1页。

〔11〕高丙中：《民间的仪式与国家的在场》，载《北京大学学报（哲学社会科学版）》2001年第1期。不过，仍有一些研究国家与社会关系的学者依然使用“国家处在社会中”或“社会中的国家”这样的表达。参见肖瑛：《从“国家与社会”到“制度与生活”：中国社会变迁研究的视角转换》，载《中国社会科学》2014年第9期；侯利文：《国家与社会：缘起、纷争与整合——兼论肖瑛〈从“国家与社会”到“制度与生活”〉》，载《社会学评论》2018年第2期。

〔12〕其他研究参见何平：《“国家在场”下的妇女地位提升——以建国初期的妇女解放为例》，载《中共宁波市委党校学报》2008年第2期；秦永章：《藏传佛教活佛转世与“国家在场”》，载《西藏研究》2020年第5期；张锦鹏、刘丽凤：《国家在场：从清代滇南盐官营看国家边疆治理》，载《云南社会科学》2021年第4期。

〔13〕〔法〕皮埃尔·布尔迪厄、〔美〕华康德：《实践与反思——反思社会学导引》，李猛、李康译，中央编译出版社1998年版，第133－134页。

〔14〕参见前引〔13〕，皮埃尔·布尔迪厄、华康德书，第156页。

米格代尔的“国家”观念借用并改编了布尔迪厄关于“场域”的界定，〔15〕而且，米氏认为：“国家不是固定不变的实体，社会也不是。他们共同在相互作用的过程中改变各自的结构、目标、规则以及社会控制。它们是持续相互影响的。”〔16〕因此，无论是组合概念还是整体概念，“国家在场”就是被建构起来的一个研究方法，用来探讨国家权力在社会领域中的存在与体现，即国家通过政策、法律、行动、仪式等方式对社会产生影响，社会采取一定的方式和策略对国家进行回应。

（二）“国家在场”引入个人信息保护的可行性与必要性

作为舶来品，“国家在场”在具体运用方面需要进行理论探讨与实践检验。〔17〕除了在民族学与社会学等领域的运用，一些学者对“国家在场”做了进一步的延伸理解与扩展运用。比如，卫跃宁用它来表达法益变迁时所坚持的一种国家本位主义，突出国家主导的优势及作用；〔18〕陈洪等学者用它来描述国家以某种形态，通过干预、分化、渗透、整合及引领等各种方式和途径参与经济和社会事务的运作；〔19〕廉睿和高鹏怀用它来透视族群法治知识以获得对民族法治现象的合理解读；〔20〕任文启用它来检讨涉罪未成年人服务个案的实践；〔21〕许超等学者用它来思考全球治理中国家的地位与作用〔22〕等。因此，对“国家在场”这一分析框架的价值挖掘，已成为学者们不谋而合的共识。

本文亦借鉴这一研究范式，试图通过研究视角上的革新，分析并反思国家如何干预、渗透、整合及引领个人信息保护实践，并寻求理念与制度上的突破。从表征上看，这是一种视角革新，在强调学科交融与知识共享的语境中，具备形式层面的可接受性。从实质上看，由于国家作用于个人信息保护领域是一个既成事实，这一分析框架可用来透视国家参与个人信息保护的实践、影响及其不足。个人信息保护作为重要的社会问题，不仅是个人、企业与政府表达利益需求的场域，而且是国家表达权威的舞台。因此，“国家在场”视角的引入，就是立足外部观察的视角，检视国家如何渗透并规范个人信息处理活动，从而实现个人信息保护与利用的平衡。换言之，本文的目的在于审视国家在个人信息保护方面的微观运作、实践影响以及后续的调整方向。

〔15〕 米格代尔放弃了韦伯关于理想型国家的界定，反而在借鉴布尔迪厄“场域”概念的基础上，认为国家是一个权力场，集观念和实践于一体。在观念上，国家是一个被公众承认的整体性组织概念，但在实践中，国家与社会之间的互动呈现出四类结果类型：一是国家渗透致使社会力量消亡或顺从的完全转型；二是国家吸纳社会力量建立统治模式，社会也影响了国家；三是社会力量吸纳国家，虽然统治模式没有变化，但国家各组成部分的面貌发生变化；四是国家在努力渗透（社会）时完全失败。参见〔美〕乔尔·米格代尔：《社会中的国家：国家与社会如何相互改变与相互构成》，李杨、郭一聪译，张长东校，江苏人民出版社 2013 年版，第 22 页。

〔16〕 前引〔15〕，乔尔·米格代尔书，第 58 页。

〔17〕 参见崔榕：《“国家在场”理论在中国的运用及发展》，载《理论月刊》2010 年第 9 期。

〔18〕 参见卫跃宁：《由“国家在场”到“社会在场”：合规不起诉实践中的法益结构研究》，载《法学杂志》2021 年第 1 期。

〔19〕 参见陈洪等：《“国家在场”视角下英国竞技体育治理实践研究》，载《体育科学》2019 年第 6 期。

〔20〕 参见前引〔9〕，廉睿、高鹏怀文；廉睿、高鹏怀、卫跃宁：《由“乡土中国”到“国家在场”——族群法治知识在民族地区社会治理中的运行机制研究》，载《社会科学战线》2017 年第 10 期。

〔21〕 参见任文启：《国家如何在场？——国家亲权视野下涉罪未成年人服务个案的实践与反思》，载《青少年犯罪问题》2020 年第 5 期。

〔22〕 参见许超：《全球治理中国家如何在场——兼与刘建军教授商榷》，载《探索与争鸣》2021 年第 8 期；任剑涛：《找回国家：全球治理中的国家凯旋》，载《探索与争鸣》2020 年第 3 期；刘建军、莫丰玮：《国家从未离场，何须找回——兼与任剑涛教授商榷》，载《探索与争鸣》2021 年第 1 期。

正是基于上述考虑，“国家在场”这一分析框架被引入个人信息保护领域，使得阐述并揭示国家与个人信息保护制度的互动成为可能。“国家在场”视角的引入主要有以下三点理由：（1）现有的个人信息保护以个人为中心来对抗企业与政府，但个人受限于认知能力和经济能力，难以应对动态化、复杂化和风险不确定的个人信息处理过程，也无法回应数据权力蕴含的技术性和资本性的基本特性。而且，个人信息保护的有效性有赖于国家规制，实践中处于维权第一线的往往是监管机构而非个人本身。〔23〕（2）国家保护个人信息具有规范基础。虽然我国《宪法》并未对个人信息保护做出明确规定，但《宪法》第33条第3款对人权保障的规定以及第38条关于公民人格尊严的强调，无不切实地指引并评价国家权力的行使。〔24〕《个人信息保护法》亦从国家层面建立个人信息保护制度，推动在政府、企业、相关社会组织和公众之间形成共同参与个人信息保护的良好环境。（3）国家介入具有强烈的现实需要。数字经济的蓬勃发展使得个人信息成为生产生活的关键环节和核心内容。各主体一方面共享某些价值追求和利益结构，另一方面却因立场、利益取向和社会角色不同而产生冲突。〔25〕但基于个人信息生成的数据权力，却被企业和政府垄断，〔26〕使得个人正处于并将长时间处于被观察、被记录与被操纵的境地。因此，需要国家以中立的姿态介入，运用多种方式或不同工具，去调整个人、企业与政府之间的互动。

三、“国家在场”视角下个人信息保护的实践与功能

个人信息保护是国家的权力实践，但国家意志的嵌入较为隐蔽，需要逐步解析国家的实践与功能，以便真切凸显“国家”的存在，进而促进对国家权威的认同。国家作为形塑力量在场，其姿态是主导者和施惠者，而政府、企业和个人则是参与者和受惠者。本部分就分别从“个人—企业—政府”的主体维度去观察并分析国家在个人信息保护实践中的在场。

（一）维护个人利益的知情同意规则

原则、规则或标准等具有表达特定思想情感、传递主流价值取向、引导规范主体行为的作用。因此，个人信息保护才会成为日常生活的公共谈资，知情同意规则才会作为信息处理最重要的合法性基础。〔27〕国家嵌入的一条路径就是通过“知情同意”规则进行多渠道、多形式的输出，使公众不自觉地成为这一规则的“传导者”和“发酵者”，完成规则主导权的“潜在让渡”和规则精神的内在化。具体而言，公众在以实用和自利为导向的生活逻辑支配下，通过直接援引部分与日常生活相近的法律文本，如《民法典》《个人信息保护法》，将“知情同意”规则结合日常经验进行再理解或转换成“近经验”，从而实现这一规则的具体化。此外，知情同意规则的力量还在于塑造主体和客体的思想和行为，即通过宣传、鼓动、强制、引导与塑造等方面的功能，帮助个人建构、维持或瓦解社会权力关系。一方面，知情同意规则有助于维护和发展个人信息自决的

〔23〕 参见张新宝：《我国个人信息保护法立法主要矛盾研讨》，载《吉林大学社会科学学报》2018年第5期。
〔24〕 参见前引〔5〕，王锡锌文。
〔25〕 参见程啸：《论我国个人信息保护法中的个人信息处理规则》，载《清华法学》2021年第3期。
〔26〕 参见前引〔5〕，王锡锌文。
〔27〕 参见王成：《个人信息民法保护的模式选择》，载《中国社会科学》2019年第6期。

理念；另一方面，知情同意规则的形成及散播方式又深刻地影响各种社会力量及其相互关系。经由知情同意规则的确立与引导，国家意志就在个人信息保护中得以彰显，扎根于“民众的集体无意识之中”〔28〕。

因为信息主体与信息处理者之间存在着信息不对称和谈判力量不均衡的情况，所以在具体规则的设计上需要对个人进行倾斜保护，以平衡信息市场中出现的非对称权力结构。知情同意规则在发展过程中，通常与国家权力相伴相生、互为增益，呈现出一种“隐秘性共谋关系”。例如在“黄某诉微信读书案”中，原告指出，微信读书没有征得原告的有效同意，而随意迁移微信好友关系，默认向未关注的微信好友公开读书信息。在“凌某某诉抖音案”中，原告预先清空了手机通讯录并拒绝软件读取，但在“可能认识的人”一栏中，抖音依然向他推荐多年未联系的同学、朋友等。在两案中，北京互联网法院均支持了原告的诉讼请求。〔29〕这就说明，当知情同意规则深入人心，会激励用户积极维权，司法体系也会及时回应。知情同意规则的承认意味着，虽然个人信息具有很强的社会性和公共性，〔30〕但个人信息自决依然是应坚持的基本理念。换言之，个人信息的处理活动需要个人参与，个人信息不能不受限制地被轻易交换和出售。

（二）约束企业行为的隐私政策

在知情同意规则指引之下，企业需要制定隐私政策以供用户选择产品和服务时参考，这是国家对企业所能提出的要求之一，也是世界多个国家和地区的通行做法。“仪式及其包含的符号是至关重要的，因为个人成为个人，社会成其为社会，国家成其为国家并不是自然天成的，而是通过文化、心理的认同而构成的，而这种认同又是通过符号和仪式的运作所造就的。”〔31〕隐私政策就是国家在保护个人信息时面向企业要求的文本实践。所谓隐私政策，是一种关于信息将如何被使用的通知形式，以及一种限制信息未来使用的默认合同承诺。〔32〕不过，它绝非透明的中性要素，而是表征了一种权力意志，即国家对于企业开展个人信息保护所持有的价值判断。因此，隐私政策被视为一种企业自我规制的工具。〔33〕当企业将个人信息保护实践公之于众时，也为行政机关提供了规制其行为的依据。〔34〕

隐私政策在个人信息保护领域中的绑定，不仅为保护个人信息注入“合法性”或部分“合法化”的国家力量，而且在借用国家力量的同时获得对企业行为的引导与塑造。比如美国联邦贸易委员会鼓励企业自我规制，自我规制在欧盟实践中也是不可或缺的组成部分。隐私政策是国家在场的文本具象，它负载着许多保护个人信息的说明与解释，而且文本的符号体系使这些描述呈现

〔28〕 申恒胜：《乡村社会中的“国家在场”》，载《理论与改革》，2007 年第 2 期，第 14 页。

〔29〕 参见《微信读书被判侵犯用户隐私“流量变现”的边界在哪里》，载 https://finance.eastmoney.com/a/202008031578777585.html，最后访问时间：2021 年 11 月 9 日。

〔30〕 参见前引〔5〕，高富平文。

〔31〕 前引〔11〕，高丙中文。

〔32〕 See Daniel J. Solove, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 *Stanford Law Review*, 1448 (2001). 其后，丹尼尔·索洛夫（Daniel J. Solove）和伍德罗·哈佐格（Woodrow Hartzog）在 2014 年发表的一篇文章中这样定义隐私政策，它是指互联网企业以在线文件的方式自愿披露其对用户个人信息保护的原则和措施。See Daniel J. Solove, Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 *Columbia Law Review*, 594 (2014).

〔33〕 See Joel R. Reidenberg et al., Privacy Harms and the Effectiveness of the Notice and Choice Framework, 11 *I/S: A Journal of Law and Policy*, 490 (2015).

〔34〕 参见高秦伟：《个人信息保护中的企业隐私政策及政府规制》，载《法商研究》2019 年第 2 期。

出某种规则和运行方向，比如企业如何收集、使用、存储和分享个人信息，如何保证信息安全，用户享有哪些权利，设置了哪些隐私功能等等。隐私政策虽然是被规定的，其功用也相对稳定，但这一切并非是固定不变的。在某些情况下，隐私政策也是变量。比如当企业变更或修订他们的隐私政策时，就应该在登录及版本更新时以推送通知、弹窗或其他符合法律要求的适当形式向个人展示变更后的指引。

（三）要求政府作为的行政规制

隐私政策合规的过程中可能出现各种各样的困境，如企业违反承诺或自身能力不足等。因此，政府作为国家意志的直接代理人有必要加以干预，通过相应的积极作为，以回应个人对个人信息保护的高度关切。这是国家对于政府所能提出的要求之一，也与域外经验相一致。比如美国联邦贸易委员会会审查相关的信息或直接联系企业，如果必要，还会向企业发出正式函件，要求提供文件和信息，进行约谈或要求作证，并可能访谈第三方。欧盟各成员国政府会审查各行业的行为规范，在确保规范内容与法律一致的情况下，还会征求信息主体和其他利害关系人的意见。〔35〕政府规制强调的是外部监督和处罚，旨在使隐私政策真正产生拘束效果。同时，由于个人信息侵权案件举证困难，政府介入可以弥补个体举证能力的不足。政府规制表征的是一种权力意志的自上而下的传达，即国家对于政府履行个人信息保护职责的行为要求和立场预设。一方面，个人信息保护充分运用了政府资源，使自身价值得到政府的正式承认和维护；另一方面，政府也从个人信息保护中收获了“政治意义和经济价值”，并最终转化为政府规制的动力。

政府规制的提倡是因为国家充分意识到在个人信息保护中，仅靠知情同意规则和企业自我规制具有难以避免的消极作用。因此，国家充分运用积极的“功能替代”策略以实现相应的保护目标。从这个意义上来说，政府规制就是个人信息保护实践的强力后盾。不过，为了确保企业创新与经济发展，政府仅在个人和企业的行为难以维护个人利益时实施其规制。政府也可以主动组织开展个人信息保护的宣传教育，对应用程序的隐私保护情况进行测评，制定个人信息保护细则与标准等。政府运用科层治理的运作逻辑，自上而下地实现对个人信息保护的控制。一方面，由国家网信部门统筹协调个人信息保护工作和相关监督管理链条，让监管责任得以层层传达与落实。另一方面，在个人信息有序保护中，个人的信息保护需求与企业的信息利用需求也得到极大满足。政府通过治理链条的逐级向下延伸，也将企业与个人隐秘地吸纳到国家权力运作的规范框架内。

四、个人信息保护领域“国家在场”的影响与局限

“国家在场”的既成事实并不意味着国家恰当有效地在场。国家可能在某一方面过度在场，而在另一方面又在场不足，从而引发个人信息保护目的与效果之间的错位。〔36〕“国家在场”的实践评价不以程度来划分，而以效果为基准，即实现对个人信息保护的“负责任关怀”（respon-

〔35〕 参见前引〔34〕，高秦伟文。

〔36〕 参见丁晓东：《个人信息私法保护的困境与出路》，载《法学研究》2018 年第 6 期。

sible care)。[37] 正如诺思所言："国家的存在是经济增长的关键，然而国家又是人为经济衰退的根源。"[38] 这在个人信息保护中也得到了印证。国家一方面推动个人信息保护在意义和内容方面的转型升级，另一方面，国家的介入也打破了个人信息利用的原有格局，产生了预期内或预期外的新问题。

（一）内容上全面兼顾但实效欠佳

虽然我们仅用了知情同意规则、企业自我规制和政府规制这三种情形表征国家在场，但这并不意味着国家仅在这些方面实现了在场。围绕个人、企业和政府这三个主体的维度，国家分别找到了具体在场的意义和价值。个人信息保护关涉的参与者主要分为个人、企业和政府这三类，[39] 因此，国家在场是全面的，且对每一主体都有相应的要求，只不过要求的兑现可能因应各种情形而呈现差异。那么各个主体兑现承诺的实际情形是怎样的呢？

其一，关于知情同意规则的实践情形。知情同意规则是个人信息处理中应该坚持的基本前提，但实质上却处于履行弱化或无能的境地。[40] 已有社会学研究证明，如果给予个人足够的信息控制能力与条件，反而增加他们披露敏感信息的意愿。也就是说，如果他们泄密的意愿增加得足够多，这种控制的增加反而会使他们更加脆弱。[41] 因此，不假思索地点击同意按钮是当下普通人的常态操作，知情同意规则只是信息处理者娴熟使用的一块遮羞布而已。

其二，关于企业隐私政策合规的实践情形。隐私政策是对法律规定的具体内化，但往往也是相对简短的承诺，是一种语法上而不是实质性的公共关系；往往是为外部消费设计的，而不是为了影响企业的内部功能。[42] 隐私政策的实践本身也存在流于形式、[43] 搭便车、规避责任以及受控于其他机会主义行为诱惑等情形。[44] 特别是，个人信息更多集中于少部分互联网企业手中，难以保证它们在信息市场上不会滥用支配地位，在非价格竞争要素的个人信息保护方面不会不当地削减服务水平。[45] 因此，隐私政策更多是企业因应法律规定和现实情势而做出的面子工程，

〔37〕"负责任关怀"是一种很高的标准，是我们对个人信息保护实践中国家有效作用的最高期待。"负责任关怀"始于 20 世纪 80 年代中期的加拿大化学品生产商协会，用以应对像博帕尔毒气泄露事件这样的严重化学品事故。负责任的关怀包括一系列自愿的行为守则，这些守则使参与的公司能够达到对环境负责任的管理的高标准。

〔38〕〔美〕道格拉斯·C·诺思：《经济史上的结构和变革》，厉以宁译，商务印书馆 2011 年版，第 25 页。

〔39〕本文为写作需要只列出了个人、企业与政府这三类主要的参与者，但个人信息保护实践中还存在一些其他的、独立的利益相关者，比如研究机构、记者和国际组织等等。有学者甚至认为数据应该被公认为"全球公域"（global commons），并被提供给所有可能的参与者加以利用以发挥数据的巨大社会价值。See Jennifer Shkabatur, The Global Commons of Data, 22 *Stanford Technology Law Review*, 354 (2019).

〔40〕比如隐私条款冗长且隐秘，专业且晦涩，个人没有时间、没有能力去阅读并理解；隐私条款简而无用，多而无功，但个人为了使用产品和服务默认同意；企业利用的内容与个人同意的内容不一致，或者超出个人同意的范围；个人信息处理的即时性特征也使得同意难以实际展开；现实中也确实存在着无须用户同意即可收集的情形等等。

〔41〕See Laura Brandimarte et al., Misplaced Confidences Privacy and the Control Paradox, 4 *Social Psychological and Personality Science*, 340 (2013).

〔42〕参见前引〔1〕，Colin Bennett、Charles Rabb 书，第 121－138 页。

〔43〕有学者分析了美国 1999 年至 2005 年间 50 家金融公司在《格雷姆—里奇—比利法》生效以来的情况，发现金融隐私通知更加完整和合规，但它们仍然能够收集大量关于客户的信息，并与关联公司广泛共享这些信息，但提供给消费者的选择并没有重大变化。See Xinguang Sheng, Lorrie Faith Cranor, An Evaluation of the Effect of US Financial Privacy Legislation Through the Analysis of Privacy Policies, 2 *I/S: A Journal of Law and Policy*, 943 (2006).

〔44〕See Dennis Hirsch, The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation? 34 *Seattle University Law Review*, 468 (2011).

〔45〕参见韩伟、李正：《反垄断法框架下的数据隐私保护》，载《中国物价》2017 年第 7 期。

纸面上的承诺与现实中的行动存在脱节。

其三，关于政府规制的实践情形。政府规制是对个人信息被侵犯的情形以及公众对隐私安全高度关切的回应。现代规制理论主张，在充分发挥市场机制和企业自我规制作用的前提下，政府规制也不能缺位。〔46〕但传统政府规制多以命令和控制为主，实施过于严格、僵化，存在阻碍创新与竞争的可能；〔47〕信息时代的政府规制又面临着平台权力、信息过载以及系统性威胁等方面的问题〔48〕。换言之，由于数据资源和处理能力的差异，政府呈现出无力通过传统治理机制作用于科技企业的算法型运作过程，由此产生治理失灵或监管真空的情况。〔49〕因此，政府规制的目标设置以及方向调整还需要进一步的细化和一致，否则就会导致行政成本上升、行动效益大打折扣，进而影响个人信息保护的治理效果。

（二）形式上规制为主但取向不明

规范个人信息处理活动是国家的核心关注。赋权与规制是个人信息保护的常用手段。不过，赋权本身受制于个人的有限性与复杂的社会现实，难以有效实现，规制反而是可欲且可及的选择。〔50〕虽然知情同意规则、企业自我规制以及政府规制都存在或多或少的问题，但国家在场的核心关切依然落脚在企业自我规制与政府规制的博弈上。个人信息保护并非保护个人对其个人信息的控制性权益，而是为了规制个人信息处理风险，防范与救济个人数据处理与利用活动可能产生的侵害后果。〔51〕

综观各国规制实践，虽然美国一再强调以自我规制为主要形态，但其政府规制也发挥了巨大作用。同样地，企业自我规制与政府规制的结合，正成为欧盟及其成员国的主要做法。〔52〕因此，企业自我规制与政府规制并非互相排斥的关系。换言之，个人信息保护实践需要企业自我规制和政府规制的合力。这两种规制之间应该是什么关系，国外学者对此莫衷一是。〔53〕有学者认为自我规制是政府规制的同义词，可根据具体情况作为政府规制的有效补充。〔54〕有学者则认为自我

〔46〕 参见前引〔34〕，高秦伟文。

〔47〕 See Jerry Louis Mashaw, David Harfst, From Command and Control to Collaboration and Deference: The Transformation of Auto Safety Regulation, 34 *Yale Journal on Regulation*, 277 (2017).

〔48〕 See Julie Cohen, The Regulatory State in the Information Age, 17 *Theoretical Inquiries in Law*, 369 (2016).

〔49〕 参见张兆曙、段君：《网络平台的治理困境与数据使用权创新：走向基于网络公民权的数据权益共享机制》，载《浙江学刊》2020年第6期。

〔50〕 当然，规制本身也不是有效保护个人信息的灵丹妙药。相反，规制通常需要在不同情况下结合不同的策略。而所有的执行都是不完美的，规则总是会被一些人违反。

〔51〕 参见王锡锌：《个人信息权益的三层构造及保护机制》，载《现代法学》2021年第5期。

〔52〕 参见前引〔34〕，高秦伟文。不过之前的研究认为，自我规制与政府规制是根本不同的实体，这意味着它们不能很好地融合。See Darren Sinclair, Self-Regulation Versus Command and Control? Beyond False Dichotomies, 19 *Law and Policy*, 530 (1997).

〔53〕 有学者根据政府干预程度的不同，将自我规制分为纯粹的自我规制、替代的自我规制和条件的自我规制；有学者则根据规制力度的渐变确立了自我规制、强制性的自我规制、自由裁量惩罚的命令规制、无自由裁量惩罚的命令规制这一规制的金字塔结构；还有的学者将自我规制分为强制的、促进的和默认支持三种类型。See Philip Eijlander, Possibilities and Constraints in the Use of Self-Regulation and Co-Regulation in Legislative Policy: Experiences in the Netherlands-Lessons to Be Learned for the EU? 9 *European Journal of Comparative Law*, 4 (2005); Ian Bartle, Peter Vass, Self-regulation within the Regulatory State: Towards a New Regulatory Paradigm? 85 *Public Administration*, 901 (2007); Ian Ayres, John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate*, Oxford University Press, 1992, p. 39.

〔54〕 See Anil K. Gupta, J. Lad Lawrence, Industry Self-Regulation: An Economic, Organizational, and Political Analysis, 8 *The Academy of Management Review*, 416 (1983).

规制是政府规制进程的一部分，必要时候还可能加强政府规制。〔55〕

根据上述讨论，自我规制与政府规制处于理论坐标的两极，中间是连续的光谱，通过调整各自的占比，以形成适应一定国情、阶段和需要的规制进路。〔56〕实证调研指出：在规制更加模糊的国家，如德国、美国，尽管文化和法律环境非常不同，但都具有最强大的企业隐私管理实践；而更受规则约束的国家，如法国和西班牙，倾向于遵从程序，而不是嵌入隐私。〔57〕那么，在我国，企业自我规制与政府规制之间应该采取何种策略呢？

目前，我国《个人信息保护法》只是将企业自我规制与政府规制的内容分别纳入“个人信息处理者的义务”和“履行个人信息保护职责的部门”的法律条文之下，未曾就两者之间如何自处与互动做更进一步的规定，也未就现阶段采取什么样的规制策略给予明确的指引，政府在个人信息领域的规制边界也难以划定。〔58〕因此，基于上述域外经验的启发与反思，在个人信息保护领域，关于我国规制策略的取向依然是一个开放的、可以继续讨论并完善的课题。

五、“国家在场”视角下个人信息保护的再造与表达

我们在前文既描述了国家的具体实践，也评价了国家实践的主要影响，并指出：国家虽然对各方主体有针对性的要求，但也未能有效地保护个人利益，维护个体尊严；虽然手段上以规制为主但也未能恰当地规范个人信息处理活动，安置好企业与政府之间的关系。因此，国家权力的参与有服务于个体权益与公共福祉的一面，但也难以避免国家在具体的制度设计或策略选择方面的缺憾。不过，所谓的不足或缺失，亦是进一步夯实国家实践的基石。

（一）理念重申：内化人性尊严

虽然法律制度和文化背景存在差异，但各国个人信息保护的立法与执法实践都证明了尊重个体是不变的坚守。换言之，人性尊严作为宪法的基本原则能够从不同的制度和文化土壤中找到依据，虽然在具体内容上各有侧重，但都是国家意志的核心表征。〔59〕因此，提倡个人信息保护，其目的在于保护个人的合法权益，使其人性尊严免于减损或矮化。重申人性尊严是对康德“任何时候以人作为目的，而不是仅仅当做手段”〔60〕观念的具体确认，也是个人信息保护实践的保护依据与行动理由，用以调整、指引或辩护人们的行动选择。“只有本人能够控制自己的个人信息，才可能自由发展个人人格。如果个人无法知晓自己的个人信息在何种程度上、被何人获得并加以

〔55〕 参见前引〔53〕，Ian Bartle、Peter Vass 文，第 890 页。

〔56〕 比格纳米（Francesca Bignami）认为，美国以透明的行政诉讼、惩罚性行政执行以及普遍的规制诉讼为主，而欧盟则以威慑导向的规制执行和企业自我规制为主。See Francesca Bignami, Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy, 59 *American Journal of Comparative Law*, 412 (2011).

〔57〕 See Kenneth A. Bamberger, Deirdre K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*, The MIT Press, 2015, pp. 12 - 14.

〔58〕 不过，在政府规制内部则体现出多主体监管的架构：一方面，国家网信部门对个人信息保护有统筹协调和监督管理的职能；另一方面，国务院有关部门、县级以上地方人民政府有关部门，在相应的职责范围内也负有监管职能。

〔59〕 参见〔德〕瓦尔特·施瓦德勒：《论人的尊严：人格的本源与生命的文化》，贺念译，人民出版社 2017 年版，第 148 - 150 页。

〔60〕〔德〕康德：《道德形而上学的奠基》（注释本），李秋零译注，中国人民大学出版社 2013 年版，第 55 页。

利用，则个人将失去作为主体参与的可能性，而沦为他人刻意操纵的信息客体，被沦为客体正是人性尊严被侵害的同义语。”〔61〕因此，个人信息保护最终针对的不是个人信息本身，也不是要限制个人信息处理，而是保护个人信息之上的自然人的人性尊严。〔62〕当个人信息之于人的人格尊严、人格自由发展价值被渐次肯定时，法律规则从充分尊重市场交易自由逐渐向维护信息主体人性尊严倾斜。〔63〕

但是，现实场景中个人的主体性地位面临的挑战日渐增加，以致人性尊严的理念指引愈发无力并衰颓。个人基本上难以从信息网络，尤其是电子化场景中抽身退出，公民习惯于命令—服从模式，因此，通过个人信息的收集和处理，个人就不再是独立的个体，而是一个个以名字、符号和标识为载体的档案，〔64〕公民生活也越来越成为可见的、可计算的、可预期的资源库〔65〕。而企业与政府不仅无法切实地践行彼此的承诺与职责，而且在某种程度上实现了共谋，共同控制个人生活以谋取私利。当个人信息遭受侵权时，由于信息处理者的技术和资本优势，私人维权面临取证难、成本高和赔偿低的困境。因此，当个人在面对强大的组织和信息处理者，在面临动态化、复杂化和不确定的过程时，更需要强化人性尊严以维护自身的独立与自主性，更需要公私机构对个人利益保持尊重和克制。正如《迈向新的数字伦理：数据、尊严和技术》报告中所指出的那样，个人信息保护相关于个人的个性发展，只有更好地尊重和保障人的尊严，才可以制衡个人面临的无所不在的监视和权力不对称。〔66〕因此，我们需要在个人与企业、个人与政府的互动中，重申人性尊严的基本理念以规范具体的信息处理行为。

重申人性尊严的价值理念，其意义表现在两个方面：首先，人性尊严理念要求公私机构的行为必须受到限制，即企业与政府应依据法定权利和法定程序收集、处理、公开与共享个人信息，否则，公民就有沦为客体的风险，难以实现信息主体的自决与自主。在信息社会，每个公民客观上已成为数据权力项下的一个“信息符号”，并被视为可以被计算、预测和控制的客体来对待。〔67〕因此，当外部侵害的风险加剧时，为防范公民成为“被处理的客体”，必须树立人性尊严理念。其次，人性尊严具体指向个人自治以及随之得到保障的不歧视（平等）、身份识别（信息的正确与完整性）、信息安全与财产利益以及社会信任等附加的实体价值与其他基本权利。〔68〕因此，个人信息保护的标准应以人为尺度，体现人的目的性，并融入人类文化之中。比如企业可以听取用户的使用建议，不直接使用“不同意即退出”的模式，而是将网络产品与服务的功能区分

〔61〕 杨芳：《个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体》，载《比较法研究》2015 年第 6 期，第 25－26 页。

〔62〕 参见前引〔51〕，王锡锌文。

〔63〕 参见郑维炜：《个人信息权的权利属性、法理基础与保护路径》，载《法制与社会发展》2020 年第 6 期。

〔64〕 See Ruth N. Cohen，*Whose File is it Anyway*，*National Center for Civil Liberties*，Civil Libertise Trust，1982，p. 10.

〔65〕 参见胡水君：《全球化背景下的国家与公民》，载《法学研究》2003 年第 3 期。

〔66〕 See European Data Protection Supervisor，Towards a New Digital Ethics：Data，Dignity and Technology，available at https://edps. europa. eu/sites/default/files/publication/15－09－11_data_ethics_en. pdf，Last visited on May 25，2021.

〔67〕 See John Cheney-Lippold，*We Are Data*：*Algorithms and the Making of Our Digital Selves*，New York University Press，2017，p. 141.

〔68〕 参见前引〔5〕，王锡锌文。

为核心业务功能和附加业务功能。〔69〕这一方面有助于吸纳新用户扩展注册信息的来源与数量，另一方面有助于老用户固着、细化关键信息的利用与共享。

正是通过这两方面的意义阐释，个人才能够真正参与到个人信息保护实践中，并从个人信息的利用中受益。因此，人性尊严的内化之于个人的重要性就在于，使个人得以找回被消解的主体性，重获参与群体生活与复杂理性活动的能力与品质。

（二）基本共识：重述规制理念

规范个人信息处理活动的首要难题并不是如何明确企业与政府之间的规制边界或设计某种规制方案，而是梳理规制背后应该坚持的主要共识，否则规制本身就是任意的或不切实际的，不仅治标不治本，而且遏制了数字红利和企业创新。那么，信息时代的规制策略应该坚守哪些共识呢？

其一，应该要求合作而不是对抗，〔70〕即以建立有序共赢的公私伙伴关系为目的。长期以来，我国的立法和实践普遍将政府规制、企业自我规制截然分开，要么放任企业恣意活动，要么由政府直接干预，突出两者的对抗而忽略合作的内涵，强调规制结果而忽略了规制的过程，导致规制效果不尽人意。〔71〕再者，企业自我规制与政府规制之间各有优劣，两者结合可能发挥更好的作用。比如巴特尔（Ian Bartle）和瓦斯（Peter Vass）根据英国近些年来的自律政策和实践指出，自我规制具有可实现的公共利益目标，虽然可能带来某些严重的系统性威胁，但可借助问责与透明的议程来实现政府规制对其的监督，以更好地实现个人数据的利用与管理。〔72〕

其二，正视市场自由化的反应，承认规制过程中的压力。在相互依存以及权力和知识分散的现代性条件下，规制不是单向的，即从公共到私人，而是私人行动者可以充当政府的监管者。〔73〕出于市场竞争或制度供给不完备的压力，因其规制者与规制对象的一体性，自我规制掌握了更多的知识与信息，从而可以找到最符合成本有效性要求的解决方案。因此，自我规制作为有效且高效的社会控制手段的正当性不能被低估。〔74〕而且，政府规制应保持自我克制的品性。一方面是因为政府规制往往具有极强的管制色彩，有可能阻碍个人信息的有效利用和增值提升。另一方面是因为政府权力运作本身受制于人力、金钱和时间等客观因素，不能想当然地“拍脑袋”决定，而是需要细致的成本收益分析。比如有学者就指出，政府规制的出场受制于无序成本与权力成本的比较。〔75〕

其三，规制应该是阶段性、动态的。“我们踩在一块完全陌生的薄冰上，很少有人了解约束

〔69〕 核心功能旨在满足用户注册产品或服务后的基本要求，附加功能则是为提升用户体验而设计。

〔70〕 参见前引〔47〕，Jerry Louis Mashaw、David Harfst 文，第 167 页。

〔71〕 参见前引〔34〕，高秦伟文。

〔72〕 参见前引〔53〕，Ian Bartle、Peter Vass 文，第 885 页。

〔73〕 See Colin Scott，Private Regulation of the Public Sector：A Neglected Facet of Contemporary Governance，29 *Journal of Law and Society*，56 (2002).

〔74〕 See Neil Gunningham，Joseph Rees，Industry Self-regulation：an Institutional Perspective，19 *Law and Policy*，363 (1997).

〔75〕 政府规制介入与否，依赖于对无序成本（disorder cost）与权力成本（dictatorship cost）的衡量。无序成本是指私人（此处指企业）损害其他人利益的能力，权力成本则是指政府或政府官员损害他人利益的能力。只有当自我规制已经无法控制无序成本时，才需要政府规制的介入。See Andrei Shleifer，Understanding Regulation，11 *European Financial Management*，443 (2005).

企业信息流动所产生的商业道德、法律问题和政治问题。"〔76〕而且，"无论是关乎私人信息保护，抑或是关乎国家安全，私人服务、公共服务和规制利益之间的界限本质上是模糊的"〔77〕。因此，我们不能僵硬地坚持某一种或混合的规制策略，而是要因应社会现实的变化增减不同规制手段的分量。传统观点认为，欧盟的规制要求过于严格，而美国的规制则较为松懈。但比格纳米的研究却发现，美国的规制较为严格精确，而欧盟的规制则趋于宽松。〔78〕因此，一国规制风格的选择并不是固定不变的，而是因时而异的。

（三）具体路径：确立回应型规制

目前，国外规制实践的共识是企业自我规制与政府规制的结合，但具体如何安排却有不同的操作。有学者基于美国和爱尔兰对 Facebook 规制措施的调查与研究，提出了回应型规制（responsive regulation）的策略，即减少对抗，拒斥传统惩罚，政府规制更多的是最后的手段。〔79〕也有学者提出企业和政府之间进行合作规制（co-regulation）的混合模式，认为这是一种可执行的、严格的方法，既能保护个人隐私，又能跟上并满足日益增长的互联网经济的需求。〔80〕无论是回应型规制还是合作规制，都不是新的现象，也面临着不少质疑。比如合作规制被认为缺乏透明和问责，以致有做空社会公共利益，并致使企业俘获政府的可能；〔81〕回应型规制也被认为增加了政府被俘获的可能性，高估了企业的理性和道德行为，削弱了人们对执法严肃性的信心〔82〕等等。

每一种规制策略都包含风险。现阶段我们需要试验并评估哪种方式是适合我国的切实有效的策略。在充满变化和不确定性的技术革新时代，我国可以确立回应型规制的阶段性选择，这既能够较好地处理信息技术发展与个人信息保护的关系，又能够有效地促进企业自我规制机制的形成与发展。与任何良好的友谊一样，回应型规制对企业和政府都有利。之所以未选择合作规制，是因为合作规制之于具体实践更多的是一个想法，而不是现实。〔83〕而回应型规制在很大程度上本身就指向企业的善意与合作，强调较少的对抗技术以调动企业积极合规的能动性来实现。〔84〕回

〔76〕〔美〕阿尔文·托夫勒：《权力的转移》，黄锦桂译，中信出版社 2018 年版，第 170 页。

〔77〕Martin Lodge，Andrea Mennicken，Reflecting on Public Service Regulation by Algorithm，in Algorithmic Regulation，in Karen Yeung，Martin Lodge ed.，*Algorithmic Regulation*，Oxford University Press，2019，p. 195.

〔78〕See Francesca Bignami，Cooperative Legalism and the Non-Americanization of European Regulatory Styles：The Case of Data Privacy，59 *American Journal of Comparative Law*，416（2011）.

〔79〕参见前引〔2〕，William McGeveran 文，第 959 页。

〔80〕合作规制又称协同规制，是指机构与行业团体或其他第三方合作，制定详细的实质性规则。这些规则随后可能成为可执行的法律，经常（虽然不总是）受到政府监管机构的批准或许可。See Dennis Hirsch，The Law and Policy of Online Privacy：Regulation，Self-Regulation，or Co-Regulation? 34 *Seattle University Law Review*，441（2011）. 艾拉·鲁宾斯坦（Ira S. Rubinstein）也主张，合作规制应该成为经济社会问题的重要思路和措施，他甚至提出了合作规制取得成功必备的五个标准：开放和透明、完整性、解决搭便车问题的策略、监督和执行，以及使用第二代设计特征。See Ira Rubinstein，Privacy and Regulatory Innovation：Moving Beyond Voluntary Codes，6 *I/S*，*A Journal of Law and Policy for the Information Society*，380（2011）.

〔81〕参见前引〔44〕，Dennis Hirsch 文，第 442 页。

〔82〕See Steve Tombs，Understanding Regulation? 11 *Social and Legal Studies*，126（2002）.

〔83〕合作规制是一个很有前途的机制，但存在重大局限性，比如受制于特定的历史文化影响，难以切实有效地达成共识。合作规制与回应型规制之间的区别主要有：（1）前者主要关注规则的内容，后者主要关注执行规则的方法，而不是规则的实质；（2）前者实践的前提是许多利益相关方达成广泛共识，后者只是影响监管机构对所有被监管实体的行为；（3）后者应用时也可着眼于合作；（4）后者切实地存在并运用着。参见前引〔2〕，William McGeveran 文，第 981 页。

〔84〕参见前引〔52〕，Darren Sinclair 文，第 534 页。

应型规制本身也可以模糊不同地区间本应明显的区别，便于有效、灵活和合作地改进现实世界的数据保护实践。〔85〕

我国的立法实践虽然没有明确我国的规制策略，但也可以从一些具体规定解读出“先自我规制后政府规制”的意味。第一，《个人信息保护法》第 58 条规定，提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行“按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督”的义务。这预示着，关于企业信息处理行为，优先适用内部合规并外部监督的行为规范策略，政府规制只在有必要的时候出场。第二，《个人信息保护法》第 61 条关于个人信息保护主管部门的职责范围，主要提及宣传教育、接受投诉与举报、组织测评并公布结果以及调查与处理违法个人信息处理活动等，这些内容不同于常规的惩罚措施，而是一种内含企业自身改进的主动引导与被动回应的治理要求。第三，《个人信息保护法》第 62 条确立了国家网信部门承担统筹协调职责。这是一种辅助性（subsidiarity）的规制形式要求，意味着政府可以不直接或间接地积极参与，但政府对大多数规制计划必须保证有某种形式的参与。即自我规制构成对政府规制的一种回应，如果企业不采取任何行动，政府就会采取行动。〔86〕第四，《个人信息保护法》第 63 条与第 64 条是关于具体监管措施的规定，从询问、调查到约谈、审计，再到移送公安机关依法处理等，从中可以看出政府的力量根据情境的轻重缓急而相应地从“督促改进到直接惩罚”发生变化。这说明，“监管机构一开始假设美德（他们应该以合作作为回应），但当他们的期望落空时，他们会以逐步惩罚和以威慑为导向的策略做出回应，直到被监管机构顺从”〔87〕。

因此，回应型规制虽然不是国家应对新现实的唯一方式，却是现阶段的一种可为的经济性选择。〔88〕一方面，回应型规制体现了规制的灵活性、包容性和敏感性，实现了多主体参与动态性规制，大大降低政府规制的成本以及避免规制失灵的问题。〔89〕比如政府主动改变直接提供保障的全能角色，转变为向企业购买服务，并鼓励和支持企业开展个人信息保护的研究、推广、宣传、培训和咨询等服务。另一方面，回应型规制实现了从外在强制到内在激励的转化。换言之，回应型规制的采用可以使政府规制的外在要求同企业保护个人信息的内在激励相容，促使企业认真对待个人信息保护实践，将个人信息保护的期望实质性地整合进工作流程中，而不是单纯停留于“如果你同意，请点击”的形式保证或避免制裁的消极应对上。

六、结　语

个人信息保护表面上围绕着个人、企业与政府之间的权利义务责任关系而展开，但其运作的背后离不开国家这一行为主体的渗透、干预、整合与引领。国家形塑个人信息保护实践主要是通

〔85〕 参见前引〔2〕，William McGeveran 文，第 959 页。

〔86〕 See Robert Baldwin, Martin Cave, Martin Lodge, *Understanding Regulation: Theory, Strategy, and Practice*, Oxford University Press, 2012, p. 138.

〔87〕 Neil Gunningham, Darren Sinclair, Integrative Regulation: A Principle-Based Approached to Environmental Policy, 24 *Law and Society Inquiry*, 864 (1999).

〔88〕 参见前引〔53〕，Ian Bartle、Peter Vass 文，第 885 页。

〔89〕 参见前引〔86〕，Robert Baldwin、Martin Cave、Martin Lodge 书，第 136－140 页。

过其对个人、企业与政府这三类主体的要求与互动而展开。知情同意规则、企业隐私政策以及政府规制这三类实践某种程度上实现了国家对个人的赋权和对企业与政府的规制。不可否认的是，这些实践仍然存在着这样或那样的现实窘境与不利因素，以至于不仅个人利益的维护大打折扣，而且企业自我规制与政府规制之间的关系取向未定。因此，需要以国家之名，重申人性尊严的理念，避免个人被视为客体；重述规制策略的共识，酝酿信息时代规制国家的行动准则；确立回应型规制，指引个人信息保护的未来议程。

Abstract：The protection and utilization of personal information involves the interests and power relations among individual，enterprise and government. State need to act as independent actor to mediate conflicts among participants and integrate personal information protection practices. The three practices of maintaining informed consent rules of individual，restricting privacy policies of enterprise and requiring administrative regulation of the government show that state presence is a fait accompli in the field of personal information protection. However，there are two problems in the practice of state presence. One is that the content gives full consideration to individual rights，enterprise responsibilities and government obligations，but the performance of each subject is not effective enough to effectively protect the legitimate interests of individual. The other is that the form is mainly to regulate the activities of information processors，but the orientation of regulation strategies is unclear，and it is difficult to properly define the relationship between enterprise self-regulation and government regulation. Therefore，the effective presence of the state in the information age needs to reaffirm the basic idea of human dignity to maintain the subject status of the individual. At the same time，the main consensus of regulation strategy is restated and responsive regulation is established to properly treat the interaction between enterprise and government.

Key Words：a state in society，personal information protection，informed consent，enterprise self-regulation，government regulation

（责任编辑：赵　真　赵建蕊）

财经法学 No. 3，2022
pp. 96 - 109

被遗忘权本土化的路径选择与规范重塑
——以《个人信息保护法》第 47 条为中心

王义坤　刘金祥*

内容提要：被遗忘权是大数据时代实现被忘却价值的一种基本方式，但也与知情权、言论自由等相关权益存在冲突。我国《个人信息保护法》没有单独规定被遗忘权，而是采取在第 47 条规定删除权制度的囊括规范方式。但被遗忘权依旧有其制度的核心价值，即消除合法公开的负面信息对个体利益和发展的不必要影响。在具体路径实现上，宜采取事后救济为主的要件个案判定方式，以信息主体案涉利益保护的正当性，以及保护方式的必要性为主要考量因素，通过对前置信息处理合法合规、主体和适用场景限定等一系列规范框架的建立，来实现被遗忘权的有限价值存在。

关键词：被遗忘权　被忘却价值　利益平衡　个人信息保护法

一、问题的提出：被遗忘权引入所导致的利益平衡困境

自 2013 年大数据时代全面来临起，大数据技术突破了人脑“遗忘易于记忆”的极限，以空前未有的方式挑战着社会对个体权益的保障。依赖网络强大的搜寻和记忆能力，个人信息痕迹广泛留存于网络空间中，他人的信息撷取与网络播散方式隐蔽、便捷且普遍，凡此种种无不使得信息主体对其个人信息的控制越发困难，致其面临着不可预料的自身权益损害。为了应对个人无法与网络超级记忆相抗衡的窘境，权利人将眼光投向侧重事前预防的被遗忘权（right to be forgotten）机制，试图以删除、禁链等方式让有负面影响的信息消失。为了应对侵袭个人权益的信息科技浪潮，欧盟沿袭其注重保障个体权益的惯例，在 2012 年欧盟《一般数据保护条例（草案）》（以下简称 GDPR 草案）中首次明确倡导被遗忘权，并在 2016 年最终通过的《一般数据保护条

* 王义坤，华东理工大学法学院助理研究员；刘金祥，华东理工大学法学院教授。

例》（以下简称 GDPR）中专设被遗忘权条款。欧盟法院在 2014 年“冈萨雷斯案”、2019 年“谷歌诉法国国家信息与自由委员会案”、2020 年“比利时谷歌案”中承认信息主体向搜索引擎主张删除信息链接的被遗忘权，更是将对被遗忘权的研究和讨论扩大到了全世界范围。

我国在有关个人信息保护的专项立法实施之前，针对被遗忘权制度的价值、引入必要性以及制度适用的利弊存在丰富的研究和理论争议。我国“被遗忘权第一案”，即“任甲玉与北京百度网讯科技有限公司人格权纠纷案”（以下简称“任某玉案”）〔1〕更是将这种理论的实践争议推向了白热化，甚至一度出现了我国否认被遗忘权制度的观点。2021 年 11 月 1 日生效的《中华人民共和国个人信息保护法》（以下简称《个保法》）也将这个问题基本定调：第 47 条个人信息处理者的删除义务以及信息主体的删除权条款已经将被遗忘权制度囊括其中，从而表明了我国个人信息立法对该舶来权利的态度。〔2〕这也是避开学界争议、从立法领域切入解决实践问题的例子，〔3〕为今后信息主体在满足法律、行政法规规定的情形下，主动要求信息处理者删除其相关信息的情形设置了基本适用依据。

在立法层面解决被遗忘权制度引入与否的问题之后，是该制度具体适用困境的解决和规范细化问题。欧盟式的被遗忘权保障模式所遇到的一系列问题，如技术障碍和成本、信息主体利益与其他所涉权益（如新闻自由、公众知情权等）的平衡，也会在我国出现。因此，如何在既有法律框架下，针对我国具体的国情，完善被遗忘权制度的本土化路径以及规范的具体细化，是本文研究的主要内容。

二、被遗忘权引入的必要性以及与现有制度的兼容

（一）被遗忘权引入的必要性：实现被忘却价值

被遗忘权制度的主要价值是解决网络环境下的忘却困境，并实现在传统社会中对个体发展有益的被忘却价值。被忘却价值与个人的人格自由发展密切相关，关系到犯错者能否重新开始生活。无法被遗忘可能会阻碍个人的健全人格发展，使其难以自主追求人生目标。例如罪犯、少年犯过去的负面记录，会致其一辈子受到社会排斥和他人歧视。为了保障行为人再社会化的人格利益，有必要涂销其前科资料，使其有改过自新的机会。〔4〕被遗忘的背后蕴含着社会宽恕行为人过错和容许其匿名生活、使其迎接全新开始、去除负面标签使其免遭伤害的意涵。“没有遗忘，就没有原谅。”〔5〕遗忘能够辅助原谅的形成，犯错者在得到社会或者被害人原谅后，较容易塑造新的社会形象。然而，大数据时代极大地扩张了被忘却价值受损害的深度和广度，需要通过被遗忘权来应对网络科技带来的新挑战。

---

〔1〕 参见北京市海淀区人民法院（2015）海民初字第 17417 号民事判决书；北京市第一中级人民法院（2015）一中民终字第 09558 号民事判决书。

〔2〕 参见程啸：《个人信息保护法理解与适用》，中国法制出版社 2021 年版，第 371 页。

〔3〕 参见刘文杰：《被遗忘权：传统元素、新语境与利益衡量》，载《法学研究》2018 年第 2 期。

〔4〕 参见刘静怡：《社群网络时代的隐私权困境：以 Facebook 为讨论对象》，载《台湾大学法学论丛》2012 年第 1 期。

〔5〕 Meg Lega Ambrose，Nicole Friess，Jill Van Matre，Seeking Digital redemption：The Future of Forgiveness in the Internet Age，29 *Santa Clara Computer & High Technology Law Review*，99，110（2012）.

首先，网络环境的恒久存储导致“往事随着时间经过而被人们遗忘”的社会传统观念失灵。在现实社会，人们受制于有限的记忆力，逐渐形成“以忘却为原则，以记忆为例外”的模式。然而在虚拟环境中，任何人的行为踪迹都会在互联网上留下永久痕迹，出现“以记住为原则，以遗忘为例外”的情形。〔6〕这种情形导致侵权后果的加重，如精神损害与名誉损害的效果长期化。个人过去的负面记录或者错误行为完整保留在网络空间，容易招致社会偏见或者他人的负面固定印象。个人无法得到他人原谅，难以获得改过机会，或者意外地被陈旧的网络信息所伤，不利于个人人格的自我发展。

其次，搜索引擎等大数据搜集、存储技术加剧了信息主体对其自身信息掌控的不确定性。信息勘测、智能汇聚、数据恢复等手段可以发掘出任何网络活动轨迹。随意公布自己信息和转载他人信息变得普遍，滥用信息的情况也日益严重。另外，数据挖掘、比对和分析的结果具有不可预测性，而且整个过程很不透明。这种资料的相互比对和交换，能够从蛛丝马迹中拼凑出某人的各种样貌，进而造成隐私泄露。〔7〕这种对元数据的多元利用具有隐秘性，从而难以被发觉。

最后，大数据时代侵蚀被忘却价值、危及个人人格的情况下，现行的隐私权、名誉权等传统法律保障机制却显现出诸多窘境。第一，隐私权保障中“个人在公共场所自愿披露的信息不属于隐私”的传统规则过于僵化。网络空间的公共领域逐渐侵入私人领域，公私领域的界限日益模糊。〔8〕公共领域的私人信息可能会转化为隐私利益，给隐私权保障带来困难。而且信息收集使用者的多元化导致管理与控制趋于困难，传播行为与损害后果之间的因果关系也不易查明。第二，名誉权保障难以规制“片段信息拼凑导致名誉受损”现象。搜索引擎、网络媒体仅能提供未必真实的片段信息，无法完整客观地呈现个人的人品与名誉。由这些片面且可能虚假的信息拼凑而成的个人形象，容易误导社会公众。当事人可能面临名誉受损、不公平对待、经济损失等损害，名誉权保障机制对此却难以规制。另外，在保障效果方面，真实信息的持久存续使得名誉侵权的后果产生变异。网络空间的可搜索性与永久存续性使得人们“随时间而遗忘”的期待落空，足以损毁个人名誉的网络信息会成为“没有时间限制”的证据，不会随着时间流逝而消灭。〔9〕个人会与过去的过错永久联结，被侵权人无从请求损害赔偿或者恢复名誉。互联网不单是个人在社群中自由开展人格的媒介，也成为人格发展的危害来源。

（二）与现有制度兼容：实现被遗忘权与相关权益的平衡

在现有法律框架下，占据主导地位的是对传统的隐私权、名誉权进行保障的规则。信息主体原则上仅能要求信息发布者、新闻媒体、搜索引擎等网络服务商限制使用而非删除信息链接。尽管在实践中部分法院有一定的弹性解释空间，但是迄今为止，并没有代表性的司法判例。鉴于传统的权利保障机制无法应对网络环境下被忘却价值和人格受损的困境，人们寻求通过被遗忘权来满足渴望在大数据时代“被遗忘”的需求。依据学者格律特的研究，被遗忘作为法律概念具有双

〔6〕 参见张勇：《个人信用信息法益及刑法保护》，载《东方法学》2019 年第 1 期。

〔7〕 See Daniel J. Solve, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, Yale University Press, 2008, p. 95.

〔8〕 参见张新宝：《信息技术的发展与隐私权保护》，载《法制与社会发展》1996 年第 5 期。

〔9〕 参见杨立新、韩煦：《被遗忘权的中国本土化及法律适用》，载《法律适用》2015 年第 2 期。

重含义：在个人层面是对个人人格开展与表现的保护，“整个社会不再将个人与特定事实相链接，给予其重新开始的机会”；在社会层面则是指“再匿名的构建”，对维护包容开放的社会秩序意义重大。这种被忘却价值的保障需求希望通过所谓“数字橡皮擦”的信息技术，自始限制在线个人信息的存储和流通。例如欧盟法院在“冈萨雷斯案”判决中，就开创性地要求搜索引擎服务者移除特定搜索结果及其链接。

被遗忘权的引入虽然会对现有制度中的一些既有权利造成影响，但这些影响可以在相互协调中化解，在任何一种权益冲突的场景中，都可以根据利益的优先性进行取舍。

首先，被遗忘权的引入会对其他公民权利造成负面影响。从用户权利保障的角度来看，在保障被遗忘权的同时如何兼顾他人的言论自由、信息取得自由、新闻自由乃是困难的法律选择，会引发严重关切。之所以言其重大，是由于被遗忘权作为人人得以修改其自身评价的技术工具，如果删除标准不透明、不合理，就可能削弱其他人接受和记忆信息的自由，妨碍民主社会的健全发展。〔10〕具体到被遗忘权的实施，资料控制者需要承担证明“存在不应删除之例外事由”的责任，还面临若不及时删除就要被高额处罚的压力，因此，其倾向于在模糊的案例中直接删除信息。这就导致被遗忘权可能恣意侵害表达自由，引发网络言论市场的寒蝉效应，阻碍社会进步与个人发展。同时，如果仅仅保护表达自由而不保护接收思想的自由，则难以实现言论自由旨在保障个人思想的目的。这就意味着在网络的众多言论中，公民可以自由选择要接触和保存何种个人记忆、集体记忆。被遗忘权删除、隐藏信息的方式必然会阻碍第三人接收、记忆某些信息的自由，因而对言论自由造成影响。从欧盟的司法实践来看，网络新闻媒体相继收到搜索引擎删除新闻链接的通知，删除的标准既不透明也不合理，不仅侵犯新闻媒体的自主性，而且直接损害社会公众的知情权。

被遗忘权作为预防他人侵犯隐私的技术措施，主要是协助预防网络监视、数位永久记忆、深入的资料比对等侵权行为。在万物联网的数字社会，所有人的日常生活随时都在生产着“后设资料”（metadata），即有关信息本身而非信息内容的资讯，如上网、通话时的发言位置、对象、通讯时间等。〔11〕在大数据技术的监控下，这些线下生活所产生的资料都可能经由收集整理而成为线上资料库的内容。其他人、企业和政府监管能够通过深度比对，轻易地辨识每一个人的身份、喜好、人际脉络、政治倾向、私密生活等细节。通过内容资料、后设资料、商业资料库、公私部门相互往来的数据、监控所得资料的积累、比对和分析，每一个资料主体在大数据监控体系下都会成为完全透明的个体。大数据技术能够将以前无法进行数字化的资料全都进行数字化，每一个人都成为量化的个体。〔12〕由于数字记忆永久留存且获取性高，每个人对被忘却的需求大幅超越以往。在这样的情况下，在言论自由和被遗忘权的价值取舍上理应偏向后者。就被遗忘权与新闻自由的冲突而言，新闻媒体基于第四权理论监督政府、传递消息、满足知情权的使命在商业化社

〔10〕 这方面的讨论，参见郑志峰：《网络社会的被遗忘权研究》，载《法商研究》2015 年第 6 期；万方：《终将被遗忘权的权利——我国引入被遗忘权的思考》，载《法学评论》2016 年第 6 期；刘艳红：《人工智能法学研究的反智化批判》，载《东方法学》2019 年第 5 期。

〔11〕 See Neil M. Richard，The Danger of Surveillance，126（7）Harvard Law Review，1939（2013）.

〔12〕 See Paul M. Schwartz，Danial J. Solove，The PII Problem：Privacy and a New Concept of Personally Identifiable Information，4 *New York Law Review*，1814（2011）.

会环境中遭到削弱，在竞逐商业利益中过度侵害个人权益。而被遗忘权通过删除过度侵犯隐私的自媒体内容和新闻报道，保障个人适度维系隐私和名声，并为个人对抗媒体滥用权利提供救济渠道。欧盟的立法者明确建立针对搜索引擎、网络新闻媒体的被遗忘权机制，为此对个人数据保护立法进行修改。对我国而言，在保障言论自由的前提下，有限接纳被遗忘权并加以严格管制，应当是一项明智选择。

其次，被遗忘权会产生造成社会公益减损的成本。有学者批评被遗忘权没有审慎考虑到信息具有存在周期、信息与社会价值的关联性，可能造成社会公共利益的减损。信息本身具有存在周期，会自然而然地促使侵害个人权益的信息慢慢消失。即便部分信息仍然存在，也无法集合成为有意义的资料。〔13〕另外还有学者指出，网络汇集的完整、真实社会资讯已经成为现代社会共享的集体记忆，确保这些集体记忆不经审查并以原始状态留存是当代人的社会责任。“人类的文化建构于记忆之上。”〔14〕其中，人类通过媒介增加自身记忆的方式属于“外部记忆”（external memory），如个人电邮。外部记忆仅具有个人特质而非公共性质，不产生被遗忘权问题。与此相对，“交互记忆”（transactive memory）则是个人与社会群体之间交互产生的记忆，反映出的是群体事件和群体认知，众多的交互记忆构筑成人类的历史。〔15〕被遗忘权若要控制交互记忆，就有可能毁坏社会全体的“交互记忆”，或者由于信息缺失而使历史记录不真实、不准确。

上述担忧可以理解，但是结论有待商榷。第一，判断信息是否具有公益性、究竟有多大的潜在价值其实是相当困难的。而另一方面，数位记忆永恒和时间轴拉长导致对个人隐私的威胁，资料传播和比对分析更扩张了个人隐私受侵害的空间。在资料对个人隐私构成现实侵害，而其未来价值无法判断的情况下一概禁止资料主体行使被遗忘权，其正当性值得质疑。第二，信息的社会价值也可能遭到扭曲。信息随着时间流逝可能与现在的情形越发不相关，对个人的描述也趋向不正确，可能会成为负面价值的信息。在此情况下，当事人关注的是信息被忘却而非正确性，需要通过删除的方式，而非更正、限制使用，才能实质解决隐私问题，将该信息重归于私人隐私。第三，对于被遗忘权危及历史保存的质疑，何种事件属于历史事件本身就很难判断，不宜因噎废食，为保护历史记忆而忽略对个人隐私的保护。因此，需要综合考虑信息干预私人隐私的严重程度、一般社会公众的普遍感受、事件的社会价值等因素，在历史保存与个人私事之间进行利益平衡。

三、被遗忘权制度的核心功能及其路径选择

（一）核心功能：消除负面信息对个体利益和发展的不必要影响

被遗忘权并非一经确立就具有清晰的概念框架，其内涵一直处于变化之中，大致包括如下三重。〔16〕一是无法被搜索的权益，即原本经过合法手段而汇聚的正确信息在经过一段时间后，变

〔13〕 See M. J. Kelly, D. Satola, The Right to be Forgotten, 1 *University of Illinois Law Review*, 1－64 (2017).

〔14〕 I. Szekely, The Right to be Forgotten and the New Archival Paradigm, in A. Hoskins ed., *The Ethics of Memory in a Digital Age*, Palgrave Macmillan, 2014, pp. 28－49.

〔15〕 参见徐凤：《人工智能算法黑箱的法律规制》，载《东方法学》2019 年第 6 期。

〔16〕 See Jeffry Rosen, The Right to be Forgotten, 6 *Stanford Law Review*, 88 (2015).

得“不相关、不适当或者不必要”，信息主体有权请求信息控制者删除该信息，突显出个人主动控制其过去经历的权利。以“冈萨雷斯案”判决为例，司法机关将难以被搜索的权利概念运用于搜索引擎服务者身上，通过移除特定搜索结果、排除强相关信息等积极方式，提高个人信息接入的难度。不过，因为原始信息来源并未从网络上消失，所以难以被搜索的权利概念似乎限缩了被遗忘权的范围。二是再度社会化，即个人得以摆脱过去社会负面信息的枷锁，再次以小白身份创造全新的社会角色与行为模式。这就意味着社会公众遗忘其过往经历。再度社会化的中心是管控个人负面信息的传播范围，如限制使用违法前科资料。三是不受限制的言论自由。言论自由的基本价值是保障个人、发展自我与实现自我。如果他人利用信息主体的过往言论对抗、束缚或者伤害本人，势必导致个人选择沉默来避免潜在损害，不愿公开发表意见。因此，被遗忘权的核心价值可以从既有理论对其本质的探讨中得以发现。

被遗忘权议题的第一个层面是其权利本质。无论是GDPR还是“冈萨雷斯案”判决，均未提及被遗忘权的权利本质究竟为何，学界对被遗忘权的本质和内涵也存在着争议，这就导致被遗忘权是由何种价值建构而出的问题存在模糊之处。目前关于被遗忘权本质的主流观点是“删除权”。删除权基于信息自决权而产生，是指“信息主体有要求信息控制者在一定期间内删除个人信息”的个人信息保护权。〔17〕删除权可以通过信息发布者事前预设信息有效期限的手段，或是事后提出信息删除请求的方式来实现。删除权为了应对大数据时代个人逐渐丧失信息掌控权的状况，赋予信息主体在特定情形下要求删除个人信息的权利。个人可以掌控信息控制者如何使用涉己信息，进而构筑起个人在虚拟世界中的身份，使其得以主宰个人存在的社会价值，按照个人认知安排生活，实现“维系个人尊严、自由发展人格”的终极目标。欧盟执委会在其2012年GDPR草案的说明中指出，被遗忘权所蕴含的本质是“请求信息控制者删除的权利”。GDPR明确将现有条款中的“删除权”标签为“被遗忘权”。学者博纳等认为被遗忘权是从GDPR的“信息最小化原则”、〔18〕“合法处理信息原则”〔19〕衍生而来，本质上属于删除权。

但是，也有学者质疑以删除权作为被遗忘权本质的局限性。归纳起来，大致包括如下几个方面的理由。第一，删除权的预防性带来局限。删除信息的权利带有预防风险的性质，在启动时往往并未出现实际损害，因此，对“一定期间删除”的把握很难做到精确及时，对删除何种期限内的信息也缺乏有效判断。〔20〕第二，删除权的内涵和判断标准不明确。只有当信息主体掌握信息的利益大于他人处理信息的利益时，才有权删除。但是利益衡量的判断标准模糊不清，导致删除权的实施僵硬、绝对化，极易被滥用。第三，强制他人删除信息缺乏有力的科技手段和法律安排。由于信息技术日新月异，信息很容易被复制，难以界定谁是信息控制者，信息的彻底删除在

〔17〕 这方面的讨论，参见前引〔3〕，刘文杰文；吴飞、傅正科：《大数据与被遗忘权》，载《浙江大学学报（人文社科版）》2015年第2期；陈吉栋：《智能合约的法律构造》，载《东方法学》2019年第3期。

〔18〕“数据最小化原则”（principle of data minimization）是指数据应当适当、相关、不超越收集目的，且在不必要时及时销毁。

〔19〕“合法处理数据原则”（principle of data）是指处理数据应当经过数据主体的同意或者符合法律规定。

〔20〕 See Minhui Xue, Gabriel Magno, Evandro Cunha, Virgilio Almeida, Keith W. Ross, The Right to be Forgotten in the Media: A Data-Driven Study, 4 *Proceedings on Privacy Entrance Technology*, 394－402 (2016).

短期内很难实现。而且，目前无法逾越“删除涉嫌侵犯他人信息自由权”的法律障碍。〔21〕

因此，有学者主张被遗忘权是由保护个人更生价值之“忘却权”（right to oblivion）演化而来。忘却权的起源可以追溯到法国人格权法上的“忘却权”概念（Droità l'oubli），亦即“让不会再浮现的过往永远沉默”。简言之，是指过时、负面的个人信息不得在未来过度伤害个人尊严、人格和名声，个人拥有不受过往记录束缚的权利。忘却权适用的场合主要是刑满释放人员为了回归社会，反对他人公开其过往的犯罪记录或者个人身份，着重保障的是“罪犯再社会化”的利益。如法国《刑法》第 133 条允许以“更生、回归社会的潜在威胁”为理由消除个人的犯罪记录，规定“任何人不得储存或者披露他人的犯罪违法记录资料，法庭审判或者档案记载除外”。在 2009 年德国“沃尔夫案”判决中，德国最高法院主张“社会受众在通常情况下对信息的需求优于当事人的人格利益和忘却权，但是报导利益将随着时间流逝而失去其合理性”〔22〕。法院强调忘却权需要弹性地考量时间和空间因素，空间转移会改变社会互动模式，而历时久远也可能使公开事件改变在空间脉络中的存在意义。当时间流逝、空间转移降低了已公开事件的公共性，当事人回归社会利益和个人隐私权已超过公共利益时，则信息就应当转回到私人空间，此时应承认忘却权。

从忘却权和删除权的概念发展来看，其有相似之处也有一定的区别。第一，权利内涵不同。前者是指“令他人作为”之权利，强制其遗忘信息，因此会同其他公民的言论自由、信息取得自由有所冲突，并导致重要的社会历史记录散失。而删除权近似于“自我行动”的权利，即允许个人掌控由信息控制者所收集、使用的个人信息，但不是允许个人任意删除所有涉己信息乃至篡改历史。第二，权利成立与否的判断不同。大数据环境下的信息获得难度由于搜索引擎技术的发展而降低，而个人信息不会由于时间流逝而灭失，个人会持续受到负面评价。因此，忘却权的判断核心是时空变迁对信息属性的影响。删除权的判断则不会受到时空因素的干扰。即便信息并未损害到信息主体，或者由于时空脉络的改变而不再产生负面影响，信息主体也仍然有权主张删除。

被遗忘权概念包括两个方面的内容：一是积极方面，即“令他人忘记自己的过往”，二是消极方面，即“避免个人被过往的负面信息所缠绕”，这两个方面的内容分别对应被遗忘权的两大权源——忘却权和删除权。这两种权源尽管具有不同的背景，但是在“维系社会价值和实现政治目标”“保障个人人格”方面的功能却存在重叠，因此，在被遗忘权议题上产生交错与结合。简言之，被遗忘权是将忘却权的实质内容和《个保法》中的删除程序融为一身。一方面，删除信息作为保护隐私的直接方式，属于忽略利益平衡的绝对权利行使，不是最合理、最符合比例原则的方式。另一方面，忘却权是权衡不同利益的手段，可以灵活地判断被遗忘权在个案中的适用合理性。由此可见，被遗忘权的本质应当是这两种权利的互相结合，共同解决信息流通和信息挖掘比对造成的威胁个体权益和发展的问题。而随着立法例的演化，这两种权利的功能逐渐转化成一种以删除权为主要表现形式的基本个人信息权益分支，很多忘却权所要体现出的显性社会功效也逐

〔21〕 See Karen Eltis, Breaking Through the Tower of Babel: A Right to be Forgotten and how Trans-systemic Thinking can Help Re-conceptualize Privacy Harm in the Age ofAnalytic, 2 *Ford Ham Intellectual Law Journal*, 69－95 (2011).

〔22〕 许炳华：《被遗忘的权利：比较法之观察》，载《东吴法律学报》2005 年第 1 期，第 150－175 页。

渐在删除权中实现。

删除权和忘却权的统一在欧洲立法实践中也得到过验证。欧盟法院在“冈萨雷斯案”判决中，从2012年GDPR草案的删除资料权推导出在“信息不适当、信息不相关、超越收集目的”的情况下，信息主体有删除信息链接的被遗忘权。据此观之，欧盟法院显然倾向于将被遗忘权定位于删除权。然而另一方面，欧盟法院又增加了利益平衡的标准，主张被遗忘权要视“信息属性、信息主体受到影响的程度、信息涉及的公共性程度”等因素，进行利益平衡后作出判断，并且强调时空因素对信息的影响。由此可见，欧盟法并不是完全以删除信息作为被遗忘权的行使手段，同时也结合了忘却权的利益衡量内涵，将消除负面信息对个体利益和发展的不必要影响作为被遗忘权制度的第一要务，只是这种功效需要通过删除的显性行为方式予以体现。

（二）路径选择：在第47条下寻求事后救济的个案判定

正是被遗忘权制度的上述功能决定了其存在的价值。被遗忘权是对大数据时代被忘却价值危机的回应，开辟出一条人格权与个人信息保护的新路径。我国同样面临着数字永恒记忆带来的被忘却价值危机，理论界对被遗忘权也高度关注，司法实务中还出现了“任某玉案”等系列判决。欧盟的实践也表明被遗忘权的建构与一国法治状况，以及社会、经济等因素密切相关，贸然承认被遗忘权恐怕不但不能实现预期效果，而且会妨碍数据产业的良性发展，阻碍其他人的言论自由、网络信息取得自由等权益。因此，中国语境下的被遗忘权受到多大程度的保障，是否需要对欧盟式的保护强度作必要调整，法律探索又如何成为制度改革的推动力，尚需进行深入探讨。

前文提到，自“任某玉案”之后，就有理论和实践观点认为中国从司法上拒绝了被遗忘权的引入和适用。其实这种观点是较为片面的，该案本身的案情特点使法院在特定情形下作出了一种较为合理的判定，但这种判定并非是在与被遗忘权制度完全契合的场景下作出的，简言之，该案中任某玉想要救济的利益，与被遗忘权核心价值所要救济的利益并不相同。我国学者也在研究中较为详细地将该案与“冈萨雷斯案”作了非常有说服力的比较。[23] 首先，信息处理者对案涉个人信息的使用目的存在差异。在“任某玉案”中，任某玉与某教育公司的相关信息是合作期间后者自我宣传的推广结果，是任某玉的真实履历。其发布的目的以及现存的价值没有变化，都是对任某玉的一段真实职业经历的具体体现。而“冈萨雷斯案”中，信息主体的个人信息出现在《先锋报》的一份清单中，目的是为了在拍卖活动中吸引更多竞价者，而之后其使用目的和必要性已经丧失。其次，信息主体的诉争权益不同。“任某玉案”的原告诉争权益是对其职业发展利益的影响，而法院经过调查后发现，这种影响以及相关信息所涉及的公众知情利益之间有着较为激烈的博弈，个体利益在本案中并非占有绝对主导性的保护优势。而在“冈萨雷斯案”中，其个人信息最初发布在一家地方上极具影响力的报媒上，只要搜索其全名就会显现当时的案涉信息，且该信息已经对原告本人在该区域的生活造成了一定侵扰，甚至对其个人尊严都构成了实质性侵害。所以法院判定案涉信息存在不当性以及遗忘的必要性。也正是因为前两个原因，才会产生如果行使被遗忘权则会对相关涉他权益产生影响的问题。概言之，被遗忘权的适用应当对特定案件中的争议权益作出具体分析和考量，如果不执行被遗忘权，对信息主体的侵害将影响其基本权益乃至

〔23〕 参见前引〔10〕，万方文。

个人正当发展，那么就应当赋予信息主体被遗忘权，同时，也需要对执行被遗忘权的社会成本予以考量，来实现本文所提出的性价比问题，即当执行被遗忘权给信息处理者或者从广义上讲这个社会的整体成本带来了不必要的负担，那么就需要慎重。例如“冈萨雷斯案”中删除与原告有关的链接不会对谷歌造成过重的负担，而“任某玉案”中则需要对搜索引擎中的关键字进行涤除，会产生额外的负担，且会对其他享有知情权并需要搜寻该资讯的人带来额外的行动成本。

综上，我国《个保法》第 47 条已经将被遗忘权制度囊括其中，且依前文所述，被遗忘权的适用范围十分狭窄，因此，只有当相关负面信息对信息主体的合法生存发展带来不必要的影响时，才应当适用被遗忘权，而这需要依据案情的特殊性具体分析该不必要的影响。欧盟法院也提出了对于被遗忘权类案件的个案化处理倾向。〔24〕 所以，个案分析以及要件认定的路径就在所难免。这也是在现有法律没有将被遗忘权独立成文的背景下，为了与一般删除权细化区分，实践必然要采用的路径。

四、被遗忘权制度本土化的规范重塑

（一）适用前提和规范兼容：在第 47 条之下寻求适用空间

在任某玉案中，任某玉的律师和主审法官都在说理部分将被遗忘权归入一般人格权的范畴中进行分析，这是基于彼时被遗忘权在我国的法律适用困境。而《个保法》第 47 条的存在使得被遗忘权可以寻求到更加“手段化”的适用条款，无需再向一般条款逃逸。根据王利明教授的观点，《个保法》所包含的关于个人信息的私法规则与《民法典》构成特别法与一般法的关系，《民法典》确立的个人信息性质及其在民事权利体系中的位置，是解释和适用《个保法》相关规则的基础和依据。换言之，《个保法》中的条款适用需要在《民法典》的框架体系中展开，其适用应当贯彻《民法典》确认的人格尊严价值，并结合《民法典》确认的人格权保护一般规则。〔25〕 因此，在《个保法》第 47 条项下寻求被遗忘权的适用空间，依旧需要遵循《民法典》中针对一般人格权的相关立法宗旨和原则，只是无需再寻求一般人格权的直接保护。

尽管被遗忘权的适用范围逐渐被删除权所覆盖，但依旧有自己独特的适用空间。如前所述，被遗忘权的适用场景为：争议信息的处理以先手合法合规性为前提，之后由于争议信息公开后体现出的不必要性、不相关性（如时效已过），对信息主体造成不合理的、不利影响的情况。而删除权适用中的争议信息有可能在一开始处理时就是违法违规的（包括自始违规和事后违规），所以删除权适用范围会更宽泛。因此，《个保法》第 47 条虽然是以信息处理者删除义务和信息主体的删除权作为规范内容，但其中涵盖的被遗忘权适用条件包括第（一）项和第（五）项，即“处理目的已经实现、无法实现或者为实现处理目的不再必要”“法律、行政法规规定的其他情形”。此时，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除。而本条中的第（二）（三）（四）项更符合删除权实现的前提。第（一）项与欧盟基本定义中“不

〔24〕 See Google Spain SL，Google Inc. v Agencia Espaola de Protección de Datos，Mario Gosteja González，C－131/12 EU：C：2014：317.

〔25〕 参见王利明：《论〈个人信息保护法〉与〈民法典〉的适用关系》，载《湖湘法学评论》2021 年第 1 期。

恰当的、过时的、于自身不利的信息”范围基本契合。即当信息处理目的已经实现、无法实现，或者为实现处理目的已经不再必要，且该类信息可能随着时间的推移变得不恰当、过时、对信息主体不利。如果满足其他个案考量要件，信息主体即可以行使被遗忘权。

即使 GDPR 第 17 条第 2 款中的被遗忘权制度，也是将适用范围设定在一个合理的限度内。我国《个保法》虽然没有像 GDPR 一样明确规定该制度，但依旧存在一定的适用限制，即应当区分广义上的删除权利和被遗忘权，且我国《网络安全法》《民法典》中也都有相关个人信息删除的适用规范。如《民法典》第 1195 条规定，网络侵权中被侵权人有权要求网络服务提供者采取删除、屏蔽、断开链接等必要措施，这就足以保证构成侵权的信息在网络上被删除。这就涉及信息主体的名誉权、隐私权等人格权或者人格尊严受到侵害时，相关信息处理者的删除义务。有人主张，当前的删除权规定是以存在违法侵权行为作为网络服务者采取删除、断开链接等措施的前提条件，并未承认信息主体在任意情形下的删除信息申请权利，因此与被遗忘权有本质差异。〔26〕

因此，《个保法》第 47 条中被遗忘权适用的前提，是其他现存法律规范对信息主体的保护都无法实现案涉权益的救济，即这是可能手段穷尽之后的最终选择。例如当信息主体人格权益、人格尊严受到侵害时，如果根据《民法典》相关侵权规范或者《网络安全法》第 47 条就可以救济，那么就不需要援引其他规范。当这些规范无法实现案涉权益救济，且案涉信息的删除场景又符合被遗忘权适用的其他条件时，才可以适用该制度。

（二）被遗忘权适用的个案判定要素及限制要件

1. 目的限定与必要原则的遵循

如前所述，被遗忘权的实现是以前置信息处理行为合法合规为前提，否则直接适用删除权，而不牵涉被遗忘权。《个保法》第 47 条规定的适用删除权的前提首先是目的限定原则与必要原则。所谓目的限定原则，是指个人信息的处理应当具有明确、合理的目的。例如，针对新闻报道中涉及对他人真实声誉的影响问题，如任某玉案，应当以适用被遗忘权所达到的最终结果是否符合正当性来考量，如果删除不良信息之后会对他人的知情利益以及后续的人身财产安全产生不必要的影响（如报名参加了任某玉的辅导班后受到损失），那么这种信息处理行为目的就不合理；反之，需要考量在被遗忘权适用过程中案涉冲突利益的取舍，根据目的合理和目的明确原则进行具体判定。

所谓必要原则，是指个人信息的处理应当与处理目的直接相关，并采取对个人权益影响最小的方式处理信息，包括收集、使用、存储最小范围的信息。被遗忘权的适用也需要以这些原则的遵循为前提，并且在处理信息的过程中出现了信息处理目的已经实现、无法实现，或者为实现处理目的不再必要，以及其他法律规定的事由，使得争议信息对信息主体造成了一定的负面影响。而这种负面影响是通过其他途径无法消除的，即前文提到的被遗忘权的实现以其他必要手段穷尽为前提。

〔26〕 参见段卫利：《被遗忘权的概念分析——以分析法学的权利理论为工具》，载《河南大学学报（社会科学版）》2018 年第5 期。

2. 权利主体和义务主体限定

在需要适用被遗忘权时，首先应当由个人信息处理者来执行被遗忘方式（如断开案涉信息链接或删除案涉信息内容）。个人信息处理者是被遗忘权的义务主体，即自主决策信息处理目的、方式的组织或个人。如果是共同处理者，即两个或者两个以上的个人信息处理者共同决定个人信息处理的目的与方式，那么其中任一个处理者都有义务执行遗忘措施。至于共同处理者内部约定如何，例如，仅约定其中一个处理者有执行遗忘措施的义务，在所不问。如果个人信息处理者存在合并、分立等情形导致案涉信息发生转移，则具体接收并控制该信息的处理者负有执行遗忘措施的义务。如果处理者向他方或者向境外提供案涉信息，提供方和接收方都负有删除的义务，个人也可以请求其删除。〔27〕

被遗忘权的权利主体，即案涉信息的信息主体。根据《个保法》第 47 条，当负有主动删除个人信息义务的信息处理者没有删除争议信息时，信息主体有权请求其删除。信息主体可以亲自行使该权利，也可以委托他人代为行使。无论是亲自行使还是委托他人行使，都应当采取书面或者可以存证的口头形式，并应当列举出案涉信息侵害其被遗忘权益的事实及理由。案涉信息控制者在收到诉求之后，在条件允许的情形下应当对诉求证据和理由进行查证，并将处理意见反馈给信息主体。信息主体不满意可以诉诸法院。除了信息主体本身自主决定委托他人代理之外，有两种情形的法定代理：第一种是当信息主体是未成年人时，《未成年人保护法》第 72 条第 2 款规定“未成年人、父母或者其他监护人要求信息处理者更正、删除未成年人个人信息的，信息处理者应当及时采取措施予以更正、删除，但法律、行政法规另有规定的除外”；第二种是当信息主体为逝者时，《个保法》第 49 条规定自然人死亡后，近亲属对死者个人信息享有“查阅、复制、更正、删除等权利”。

3. 遗忘场景及条件的限定

如前所述，被遗忘权作为难以被搜索的权利，其内涵并不限于删除不相关、过时、不必要信息，还包括在特定领域限制信息主体过往负面信息的披露和使用。这种保护路径属于个人信息权益保护的事后救济路径，更加关注信息主体重新塑造身份和周身舆论的自由。我国针对被遗忘权的理论探讨日趋保守。当然，已有一些学者指出我国法律法规中广泛存在着与被遗忘权内涵相近的删除权规定，这些既有规范足以代替被遗忘权来保障人格权。〔28〕司法实践则直接规避被遗忘权的理论争议，从人格权理论领域切入建立司法判断基准。可以看到，如果需要在司法个案中实现被遗忘权，必须具备两个限定要件：首先，对信息主体案涉争议的权益保护是必要的（即利益保护的正当性）；其次，这种保护可以且仅能够通过被遗忘权实现（即保护方式的必要性）。如前文所述，需要争议信息给信息主体带来了不必要的负面影响，且这种负面影响的消除不会对其他权益的实现造成障碍。如“冈萨雷斯案”中的案涉利益，其负面影响已经严重影响了信息主体的自我发展，而反观“任某玉案”中的信息主体的发展利益与其他权益（知情权）的比较，这种发展利益的保护是不必要的。在保护方式的必要性上，除了权益保护的其他手段穷尽之外，采取被

〔27〕 参见前引〔2〕，程啸书，第 361 页。

〔28〕 参见江溯：《自动化决策、刑事司法与算法规制——由卢米斯案引发的思考》，载《东方法学》2020 年第 3 期。

遗忘权能够切实实现这种保护。

除了以上适用场景的基本限制之外，欧盟被遗忘权的执行情况也可以提供一些经验。首先是对数据市场发展的影响。GDPR 对搜索引擎服务者、电商平台、社交平台等设置了严格的合规要求和高额罚款，使得企业的运营成本大幅攀升。现阶段我国大数据产业刚起步，从经济和效率的角度来讲，被遗忘权的执行要与信息处理者履行义务的成本相协调。〔29〕不能因为承担过于苛刻的合规成本，阻碍我国现阶段相关产业的良性发展。“冈萨雷斯案”后，要求实现被遗忘权的诉求非常多，〔30〕如果不符合以上讨论的筛选要件，就会无形中加重社会不必要成本。其次是技术障碍及其克服。在大数据环境下，第三方对数据的拷贝、传播成本低廉，方式便捷，数据一经公开就难以杜绝他人的传播，且难以发现和删除，发布者的掌控权完全丧失。若要以删除网页的方式主张被遗忘权保护，几乎是不可能的任务。例如有报道称，在欧盟删除搜索引擎链接而不删除元数据网页的情况下，只要更换检索词就能够轻易获得相关信息。〔31〕欧洲网络信息安全机构提出“不能完全阻止网络用户未经授权的复制和传播行为”乃是被遗忘权面临的最大难题。〔32〕最后是法定数据留存期间的制度缺失问题。目前关于信息留存的期限缺乏规范化依据。例如，《网络安全法》规定网络服务商对网络日志的留存期限是 6 个月以上。《征信业管理条例》要求征信机构对个人不良信息的保存期限为 5 年。《网络交易监督管理办法》中规定交易信息的保存时间自交易完成之日起不少于 3 年。当处理个人信息的目的已经达到，信息主体要求信息控制者删除个人信息时，在法定的信息留存期限内，信息控制者有合法的抗辩事由，这将对用户维权产生直接影响。所以，法律另有时间期限的，也属于遗忘措施执行的考量因素。

4. 遗忘措施的执行与保障

法律需要合理界定被遗忘权的保障方式，才能有效促进相关信息主体和信息控制者间的交往，同时避免被遗忘权造成“网络空间自由的终结”。关于被遗忘权的执行是否具有域外效力，在 2019 年“谷歌诉法国国家信息与自由委员会案”判决中，〔33〕法院认为，被遗忘权不具备域外效力。法院首先提出 GDPR 并未明确禁止搜索引擎服务者监督、阻止访问或删除违反欧盟法律的信息，因此，欧盟成员国的相关机关向其提出的删除命令在法理上不受领土范围的限制，可及于“全世界的相关用户”。但是，法院接下来采取结果取向的论证方式，主张如果贸然给予谷歌等企

〔29〕 See Breznitz D. Delete, The Virtue of Forgetting in the Digital Age, 28 (3) *Review of Policy Research*, 307 - 308 (2011).

〔30〕 从 2014 年 5 月西班牙谷歌案之后至该年年末，谷歌在全世界范围内收到了公民行使被遗忘权而发出的对 498737 条链接的投诉，并成功移除了其中 41.8%。See Global Data Hub Google Spain and the “Right to be Forgotten”, available at http://unitedkingdom.taylorwessing.com/globaldatahub/article_2014_google_spain.html, last visited on Sept. 10, 2020.

〔31〕 参见丁晓东：《被遗忘权的基本原理与场景化界定》，载《清华法学》2018 年第 6 期。

〔32〕 See George Christou, Problems with the EU's proposed “Right to Be Forgotten”, 11 *Information Security*, 38 - 42 (2012).

〔33〕 法国国家信息与自由委员会在 2015 年的一起案件中，认为搜索引擎的姓名搜寻服务使信息扩散到全球而冲击信息主体的被遗忘权，因此要求谷歌删除当事人在全球网络上的系争信息链接。谷歌则以欧盟域外不适用《欧洲一般数据保护规则》为由拒绝履行，并且遭到 10 万欧元的罚款。双方围绕被遗忘权保护范围是否超出欧盟范围的争议，一直上诉到欧洲法院。See CNIL, CNIL Satisfied with Draft European Parliament Report on the Regulation Proposed by the European Commission (Jan. 16, 2020), available at https://www.cnil.fr/en/cnil-satisfied-draft-european-parliament-report-regulation-proposed-european-commission, last visited on Aug. 25, 2021.

业以全球性移除义务，则可能会出现该命令与其他国家的国内法相互冲突的局面。法院同时指出，不要求也不禁止搜索引擎服务者删除欧盟域外的链接结果，暗示在司法实务中仍有灵活空间。

至于遗忘措施的有效性，2020 年“比利时谷歌案”判决可以为我们带来一些启发。在本案中，某公民在 2019 年申请比利时谷歌公司删除与其有关的新闻报道网页链接和过期网页，但是遭到谷歌拒绝。比利时个人信息保护局在接受公民申诉后，以违反 GDPR 为由对比利时谷歌公司处以 60 万欧元的罚款，并且要求其清晰说明被遗忘权监管的职责分配情况。双方围绕被遗忘权保护范围、删除决定是否通知原始网页管理者的争议，一直上诉到欧洲法院。法院作出如下裁决：第一，谷歌的删除表格信息不完整、不透明且不精确，而且对删除的网址作了狭隘的不当解释，未能完全履行搜索引擎的保障义务。第二，谷歌的删除程序要求将删除通知相关的原始网页管理者，这种做法可能误导公民认为被遗忘权保障需要征求原始网页管理者的同意，进而降低公民请求被遗忘权保障的积极性。上述做法均违反 GDPR 第 5 条有关“个人信息处理应当具有合法性、公正性、透明性”的原则要求。

欧盟信息委员会（EDPB）在 2020 年 7 月颁布《欧盟被遗忘权在搜索引擎案件中的保障指南》，总结归纳 GDPR 生效五年以来的实践经验，对被遗忘权的保障规则进行解释细化。主要内容包括：第一，公民向搜索引擎等个人信息处理者提出删除的理由。该文件对 GDPR 第 17 条的内涵作详尽描述，如由公司持有之有关他或她的数据已从公开信息中删除，公司网站的连结中包含离职员工的信息主体联络方式，或者个人信息的在线储存时间已超过法定期限，此类情形均可申请删除。此外，个人信息处理者需要将删除请求告知第三方，旨在赋予原始控制者更大责任。第二，明确拒绝删除的例外情形，包括为履行法定义务、公共利益或为行使公权力而执行的任务。〔34〕

实践表明，欧盟式的被遗忘权保障方式具有两项特征。在落实手段方面，是以“隐藏信息摘要”而非“完全删除信息”为主。公民不必通过完全删除网络空间的相关信息，而是通过要求搜索引擎等网络服务商删除搜索链接、隐藏信息链接摘要、屏蔽信息主体的身份等“隐藏”方式，来实现保障被遗忘权的目的。这种方式既能保障公民被遗忘权的实现，也不会对社会公共利益、他人的信息流通自由造成过度侵害。此即所谓相对化的遗忘，并且是在必要时，有权机关（主要是公权力机关）可以通过技术手段进入后台查验的一种遗忘。信息主体所期待达到的目的并非网络世界的绝对遗忘，这种遗忘也并不现实，而是一种在正常网络社交领域和线下社会氛围内的相对遗忘，使得信息主体可以在这样的环境中消除该信息给其带来的不必要困扰。网络服务商、新闻网站等需要回应信息主体而删除链接的“去列表权”，而非要求其永久地对所有信息负责。在权衡结果方面，具有个人信息保护优先的衡量取向。信息主体的被遗忘权不仅优先于搜索引擎服务者的经济利益，也优先于社会公众通过搜索取得信息的利益。尤其是当原始网页发布的信息并不具有违法情形时，法院往往是根据个人信息的重要性径行判定搜索引擎服务者具有隐藏搜索结

〔34〕 See EDPB, Guidelines 5/2019 on the Criteria of the Right to be Forgotten in the Search Engines Cases under the GDPR (part 1).

果的义务。对不同的案涉信息采取何种方式的遗忘，应当以具体适用场景为准，并以对案涉相关权益的损害最小化为必要考量标准。

五、结　语

大数据社会的个人不仅想要被记住，也想要被忘却。被遗忘权有望使大数据时代的人格权和个人信息保障模式发生颠覆性变革。信息主体通过删除和隐藏侵害个人隐私、名誉的信息来重新建构“忘却”的自然属性，让被忘却价值在大数据环境下得以存续，并且弥补传统个人权益保障机制的不足。被遗忘权的确有妨碍他人言论自由、信息获得自由和新闻自由，不利于历史保存价值，减损社会公共利益等缺陷，但是只要保持制度适用的范围限制，就不失为一种恰当的权利保障方式。在《个保法》实施的当下，基于我国国情，在删除权的基础上努力为被遗忘权探寻出一种不可替代的适用价值，并选择事后个案判定的路径，不失为一种对忘却价值的尊重与实践。

Abstract：The right to be forgotten is a basic way to realize the value of being forgotten in the era of big data，and there is a conflict between the right to be forgotten and the rights and interests related to the right to know and freedom of speech. The Personal Information Protection Law of China does not prescribe the right to be forgotten separately，but adopt the way of including it in the deletion right of the Article 47. But the right to be forgotten still has its core value，which is to eliminate the unnecessary impact of legal disclosure of negative information on individual interests and development. About the concrete approach of realization，it is appropriate to adopt the method of judging the main elements ex post，considering mainly the justification of interest protection，and the necessity of protection. The realization of the limited existence value of the right to be forgotten needs the establishment of a series of normative frameworks，such as the legal and regulatory framework for the pre-processing of information，subject and applicable scene qualification.

Key Words：right to be forgotten，forgotten value，balance of interests，personal information protection law

（责任编辑：殷秋实　赵建蕊）

财经法学 No. 4，2022
pp. 51 - 66

论个人信息侵权中的损害

朱晓峰　夏　爽*

内容提要：数字时代中个人信息侵害引发的特定风险具有不可逆性、不可测性和扩散性的特点，在侵害后果发生之前将这些风险认定为法律上的损害并通过侵权法予以救济，可以将侵权行为的成本内部化，既能发挥预防作用以实现帕累托最优，又能实现侵权法的震慑作用。对此，应当以规范损害说修正差额说，将满足特定条件的风险作为损害纳入侵权法上的可赔损害范畴，与财产损失、精神损害一样获得侵权法的救济。在风险性损害的具体认定上，应建立动态的评价体系，由法官在个案中综合考虑涉案的各考量因素进行利益权衡后确定。

关键词：个人信息侵权　差额说　规范损害说　风险社会　风险性损害

一、问题的提出

我们生活在个人信息可以广泛共享的时代，互联网平台将其掌握的海量兼具广度和深度的个人信息用于用户分析、精准广告投放；在虚拟货币加持下，不可控的暗网论坛等社交平台正成为信息贩卖的渠道；随处可见的身份绑定、过度索权加大了使用 APP 导致的个人信息泄露风险。根据《2021 年 App 个人信息使用态势分析报告》，在近 1 万款活跃的 APP 应用当中，有 56.3％的应用涉嫌非法收集和使用个人信息，64.6％的应用涉嫌“未经用户同意收集和使用个人信息”。〔1〕然而，与频繁发生的个人信息侵权事件形成鲜明对比的是，在个人信息侵权案件中，受害人主张侵权损害赔偿却并不容易。司法实践中，因原告无法举证证明实际损失而被驳

* 朱晓峰，中央财经大学法学院教授；夏爽，中国人民大学法学院硕士研究生。
本文为国家社会科学基金重大项目“大数据法制立法方案研究”（18ZDA136）的阶段性成果。

〔1〕 参见《2021 年 App 个人信息使用态势分析报告》，载 https://www.donews.com/news/detail/4/3152878.html，最后访问时间：2022 年 4 月 5 日。

回诉讼请求，并不鲜见。〔2〕导致这一悖论出现的重要因素之一是证成侵权责任成立所需的损害要件存在困难。〔3〕

在个人信息侵权案件中，受害人遭受不利益的情形既包括侵权行为人窃取个人信息后实行诈骗等行为而使受害人遭受财产损失，或者受害人隐私被非法泄露后而遭受精神损害，也包括各种难以纳入财产损失和精神损害范畴的新损害类型，例如，因个人信息泄露而引发的可能在未来转化为现实损害的风险，或担心因个人信息泄露导致不利后果而产生的焦虑等。对此，《个人信息保护法》第 69 条第 2 款只规定了确定损害赔偿额的三种方法，并没有关于个人信息泄露等情形所导致的风险是否可以纳入侵权法上损害范畴的直接规定。而《民法典》规定的侵权法上的可赔损害通常包括财产损失和精神损害，也没有将风险作为损害的明确规定。事实上，与《个人信息保护法》《民法典》规定的典型可赔损害类型相比，个人信息权益被侵害后所引发的一系列风险确实更具不确定性、难以计量性、无形性等特征，〔4〕受害人因侵害行为而承受“风险”时，通常并没有遭受现实财产减少的不利益，而只是发生了未来财产减少的可能性。因此，如果是依据界定财产损失和精神损害的方法来认定个人信息侵害引发的风险是否属于侵权法上的可赔损害，可能无法为受害人提供充分的救济。为了解决个人信息权益侵害中损害界定难的问题，学理上有“以风险作为损害”的革新损害概念的观点，〔5〕但是，反对观点却认为这些损害难以被传统的侵权法接受而拒绝将之纳入现行法律体系内。〔6〕鉴于此，本文将讨论的问题聚焦于：现行法上的损害是什么；个人信息侵权案件中哪些损害可被认定为侵权法上的可赔损害；尤其是“风险性损害”能否在现行法框架下被认定为独立于财产损失和精神损害而被纳入侵权可赔损害范畴；如果能，又应以何种标准和方式确定这种风险导致的损害。笔者期望以此来回应当前理论与实践中关于个人信息侵权中损害认定的分歧，助益于个人信息的保护。

二、现行侵权法中损害概念的界定及修正

侵权法的首要职能是填补损害。〔7〕损害作为侵权损害赔偿责任成立的核心构成要件，一直占据基础性地位。何谓损害？如何认定损害？这些问题无论在现行法律规范的实践运用中还是在理论研究上都是一个基础性问题。如今，这一问题在层出不穷的个人信息侵权案件中又开始被重新提起，亟需重新界定。

---

〔2〕 参见北京市第二中级人民法院（2020）京 02 民终 10179 号民事判决书；上海市第二中级人民法院（2019）沪 02 民终 717 号民事判决书；天津市第二中级人民法院（2020）津 02 民终 4520 号民事判决书；浙江省嘉兴市中级人民法院（2019）浙 04 民终 3244 号民事判决书。在比较法上，美国联邦最高法院在 Clapper v. Amnesty（2013）案中明确指出，个人信息保护的诉讼请求必须证明存在客观实际的损害，“推测的”或“假设的”损害都不能得到法院支持。See Kristen Choi，Clapper v. Amnesty International USA：Balancing National Security and Individuals' Privacy，34（2）*Journal of the National Association of Administrative Law Judiciary* 444，444（2014）.

〔3〕 参见叶名怡：《个人信息的侵权法保护》，载《法学研究》2018 年第 4 期。

〔4〕 参见谢鸿飞：《个人信息泄露侵权责任构成中的“损害”——兼论风险社会中损害的观念化》，载《国家检察官学院学报》2021 年第 5 期。

〔5〕 参见田野：《风险作为损害：大数据时代侵权“损害”概念的革新》，载《政治与法律》2021 年第 10 期。

〔6〕 参见陈吉栋：《个人信息的侵权救济》，载《交大法学》2019 年第 4 期。

〔7〕 参见王泽鉴：《侵权行为》，北京大学出版社 2016 年版，第 175－176 页。

（一）我国现行法中的损害概念

考虑到损害的复杂性，各国民法典对于损害的内涵及其认定给予了不同规定，如《奥地利民法典》即明确规定了损害的概念，将损害定义为受害人的财产、权利或人身遭受的不利益。与《侵权责任法》第6条第1款相比，《民法典》在损害与侵害概念之间作了区分，〔8〕并且在损害与赔偿之间建立了规范联系，〔9〕但其并未明确损害概念的内涵。从《民法典》及相关司法解释来看，我国现行法律体系中的损害类型包括财产损失和精神损害，后者必须达到“严重”程度才可以获得赔偿。〔10〕据此，我国学理与实务上普遍认为，我国现行侵权责任法上已经构建起了固定的损害类型及项目，法官只需要对具体案件中的损害类型进行判断，再适用各自的损害赔偿项目即可。〔11〕对此，学理上有观点指出，随着损害的计算方法日益先进，统一的损害概念及其相关的上位理论似乎已经失去了实用性。〔12〕但本文认为，现行法对于损害类型及与之相对应的赔偿项目进行详细规定的核心目的在于简化司法实践中法官认定损害及确定赔偿金额的难度，而非以此取代损害概念本身。随着社会实践的不断发展，新损害类型会不断涌现，要判断这些新的损害类型是否可以被纳入侵权法上的可赔损害范畴，并不能当然以其是否能被现行法中的损害类型所囊括作为判断标准，毕竟现行法规定不同损害类型并确定相应的可赔项目，仅仅是出于对既往经验的总结而无法充分涵括未来可能发生的情形。以个人信息侵权为例，侵害个人信息可能导致各类下游犯罪的风险提高、加重社会分选和歧视、加剧消费操纵和关系操纵，并使受害者因此引发严重焦虑与不安等。若是以现行法规定的具体损害类型为标准进行判断，很难将权利人遭受的这些不利益纳入现行法上的可赔损害范畴。因此，对于个人信息侵害中的损害认定，仍有必要回归损害概念本身，继续讨论在具体损害项目之上的损害概念，以及损害认定背后的内在法律思想，从而解决将风险作为损害的理论难题。

（二）损害概念的内核：差额说及其修正

在对损害本质的认识问题上，传统损害赔偿理论主要经历了差额说、客观损害说、规范损害说的发展演变。其中，差额说一直居于通说地位，其他学说则作为差额说的修正而存在。在差额说中，损害是指财产的实际状态与损害事件未发生时财产状态之间的差额。〔13〕差额说基于完全赔偿的理念，坚持认为应在金钱价值层面将受害人的状态恢复到损害并未发生时的假设状态，在具体适用时也具有简便明了的优点，因此其一经提出便为学界和司法实践所接受。

然而，差额并不等同于损害本身，作为损害是否存在的认定方法，差额说具有一定的局限性，在实践中经常会遭遇如下难题：其一，当介入因素使原有侵权行为导致的损害被填补，应有的利益差额被其他因素抵消，如亲属看护未收费用和雇主持续支付工资，若按照差额说来认定损

〔8〕 有学者据此进一步指出，侵害权益是侵害民事权益的客观事实，损害是侵害权益的进一步法律后果。参见程啸：《侵权责任法》，法律出版社2021年版，第214页。

〔9〕 参见程啸：《中国民法典侵权责任编的创新与发展》，载《中国法律评论》2020年第3期。

〔10〕 参见《民法典》第1183条。

〔11〕 参见李昊：《损害概念的变迁及类型建构——以民法典侵权责任编的编纂为视角》，载《法学》2019年第2期。

〔12〕 参见陈聪富：《人身侵害之损害概念》，载《台大法学论丛》2006年第1期。

〔13〕 参见徐建刚：《〈民法典〉背景下损害概念渊流论》，载《财经法学》2021年第2期。

害，则难免得出并无损害的荒谬结论；〔14〕其二，财产在计算上的差额虽未发生，但却实际发生了价值上的减损，如物的商业价值的贬损将影响其未来交易所获利益，但这种不利益却未在现在发生。〔15〕亦即言，在前述两种情形当中，若按照差额说的观点，既然受害人在侵害行为发生前后并未出现财产计算上的差额，自然就没有损害，因此也无法得到金钱赔偿的救济。事实上，虽然受害人遭受的前述不利益无法转化为既有财产的减少，但受害人在侵害行为前后所处的实际状态和地位却发生了实质性的变化，这种状态上的变化是确定的、可以用金钱衡量的。而差额说则将受害人于此遭受的不利益完全排除出了侵权法上的损害范畴并拒绝予以赔偿，显然有失偏颇。差额说之所以会面临如此困境，是因为损害本身具有规范属性，而差额说却是去价值化的。损害赔偿在本质上是立法者对损失进行分配的问题，其背后是对各种价值利益的衡量和取舍。〔16〕差额说以侵权行为发生后的现存财产状况和应然财产状况之间的差额作为损害，这固然不失为对现实中异常复杂的损害的一种简便认定方式，并在绝大多数情形下符合立法者的规范意图和价值取舍，却难以避免在个别情形下无法承载立法者所有的价值立场，因此对差额说应予适当修正。

在此背景下，客观损害说与规范损害说在承认差额说基本立场的基础上，对其存在的缺陷作了必要修正。客观损害说并不把损害概念等同于受害人在侵害行为发生前后所享之利益的整体抽象差额，而是认为损害直接表现为对事物的损害、剥夺、身体伤害等具体形式。〔17〕在强调整体利益差额的差额说下，当其他介入因素的发生导致受害人的实际利益并未受到减损时，侵害行为人便可避开对受害人的赔偿，而客观损害说则可以避免差额说这一不足。规范损害赔偿理论强调损害赔偿在计算时不仅要考虑侵害行为发生前后受害人利益状态的差异，还要考虑规范目的，在损失的计算中要包括法律价值的评估。〔18〕该观点强调损害的确定是一个价值评估的过程，而不是一个简单的自然事实，据此，被害人是否受到损害的实质就是法律规范所保护的利益是否受到损害，或受法律保护的状态是否不同。〔19〕规范损害说的提出是为了在不发生差额的例外情况下承认损害的存在，从而实现对受害人的保护。〔20〕进而言之，损害的本质是当事人遭受的不利益本身，〔21〕这种不利益通常可以通过差额说的认定方法来判断；对于差额说在认定中存在的问题，可以通过客观损害说和规范损害说来解决。

在我国现行法框架下，受害人因侵害行为所遭受的不利益既可以是财产损失，也可以是精神损害。其中，财产损失主要通过差额说的方法来确定，主要赔偿实际损失；精神损害虽然是无形的、难以确定的，无法用财产上的差额进行评价，但这种难以用金钱评价的特性并不影响其可赔性，因为在差额说的修正观点即规范损害说中，损害在本质上也是规范的概念，损害的确定是

〔14〕 参见前引〔7〕，王泽鉴书，第 142 页。

〔15〕 参见徐建刚：《论使用可能性丧失的损害赔偿》，载《法商研究》2018 年第 2 期。

〔16〕 参见前引〔15〕，徐建刚文。

〔17〕 参见曾世雄：《损害赔偿法原理》，中国政法大学出版社 2001 年版，第 119－120 页。

〔18〕 参见姚辉、邱鹏：《侵权行为法上损害概念的梳理与抉择》，载陈小君主编：《私法研究》第 7 卷，法律出版社 2009 年版，第 30－45 页。

〔19〕 参见王志刚：《论民法上的损害概念的形成视角》，载《法学杂志》2008 年第 5 期。

〔20〕 参见前引〔13〕，徐建刚文。

〔21〕 参见前引〔12〕，陈聪富文。

“质性评价”，所以《民法典》侵权责任编在承认精神损害存在的基础上，将精神损害赔偿数额难以确定的问题交由法官酌定。另外，即使在人身权益侵害导致的财产损失认定问题上，《民法典》第1182条等也规定了在实际损失、侵权人获利均无法确定时，由法院根据实际情况酌定赔偿额。这实质上表明，我国现行法框架下对损害的基本认识是围绕法律保护的地位或状态是否因侵害行为遭受不利益展开：当受害人遭受了可以用财产的一般等价物货币进行衡量的不利益时，若此种不利益具有确定性，应以侵害行为前后的财产利益差额即实际损失为标准确定可予赔偿的损害；若此种不利益具有不确定性，但属于法律明确应予赔偿的范围，则可依据实际损失的替代标准如侵权人获益或者法官酌定方法确定可予赔偿的损害；当受害人遭受了不可用货币衡量的不利益时，若此种不利益属于法律明确应予保护的范围，则由法官在个案中综合考量涉案因素确定可予赔偿的损害。在第一种情形下，侵权法上可予赔偿的损害可以依差额说认定，在第二种与第三种情形下，侵权法上可予赔偿的损害应依客观损害说或规范损害说作为差额说的补充来认定。在此意义上，将个人信息侵害中受害人遭受的不利益，特别是实际财产损失和严重精神损害之外的其他不利益纳入现行法上的可赔损害类型范围，存在着可以解释的理论基础和规范空间。

三、个人信息侵权中的损害类型及风险性损害的引入

个人信息权益侵害案件中受害人可能遭受财产损失或精神损害，最常见的情况是通过购买互联网平台用户的个人信息进行诈骗导致受害人财产损失，或者通过发送垃圾信息破坏个人生活安宁，使其遭受精神损害。在这两种情形中，受害人所遭受的损害及对这些损害的侵权法上的救济，与一般侵权案件相同。除此之外，个人信息侵权案件中受害人还可能遭受新型损害。对这些新型损害，无论是在司法裁判中，〔22〕还是在域内外学理讨论上，相应的分歧均集中在因个人信息侵害导致的风险是否属于侵权法上的损害及其认定问题上。对于这些风险，可以归纳为如下几种类型：

一是个人信息泄露导致未来下游犯罪的风险剧增。如今各大网络平台掌握海量个人信息，这些个人信息往往在平台知情或不知情的情形下被攻破、盗用、收买、交易。一旦这些数据脱离合法处理者的控制范围而被不法分子利用，个人信息权人即可能会遭受他人敲诈勒索、网络攻击等风险。〔23〕

二是社会分选与歧视，即社会上的特定组织、个人可能根据个人信息中的年龄、经济实力等将自然人进行分类，并在此基础上对自然人进行区别对待或者歧视对待。〔24〕例如，低收入者必须承受更高的贷款利率，特定性别、婚育状况的求职者本应将自身状况作为隐私而不予透露，而雇主却非法获取了这些个人信息从而造成了就业市场的不当歧视，等等。

〔22〕 参见“北京蓝娃娃教育科技有限公司与吴文雯因服务合同纠纷案”，北京市第一中级人民法院（2017）京01民终579号民事判决书。

〔23〕 参见前引〔4〕，谢鸿飞文。

〔24〕 See David Lyon, Surveillance as Social Sorting: Computer Codes and Mobile Bodies, in David Lyon ed., *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge, 2002, p.13.

三是消费操纵和关系控制，如商家精准投放广告给特定受众，从而操纵购买者的消费冲动。有些平台和组织甚至通过对个人信息的精确控制来操纵其自主作出的决定，对受害者造成潜在的、甚至通常情形下无法被其认识到的伤害。〔25〕

四是受害人因个人信息泄露导致人身、财产权益遭受不确定的风险而产生焦虑与不安全感。受害人可能因为个人信息被泄露后无法掌控风险，从而处于无法摆脱的精神焦虑之中，这种精神焦虑并非基于财产或者人身权益被侵害而遭受的现实损害，而仅仅是对于未来风险的担忧，这能否被认定为现行法中的“严重的精神损害”，尚需进一步讨论。

前述风险在传统的侵权场景中并不常见，但随着个人信息被泄露和不法利用的情形逐渐加剧，这些不利益却很可能降临到社会中的任何一个人身上。受害人遭受的这些不利益通常并不表现为现实的财产减少，而仅仅表现为可能会发生的风险，但这些风险又会现实地影响每个受害人的生活，使受害人的利益状态发生显著的改变。在此背景下，这样的风险有无必要纳入侵权法的调整范畴？

（一）将风险作为损害的必要性

我们生活在信息技术向纵深发展的数字时代，自然人个人信息泄露事件频发，侵害个人信息权益的风险已经呈现出逐渐加剧的态势，风险社会理论也随之复兴。该理论认为，后工业时代人类社会的风险来源已由自然风险转变为人为风险。〔26〕其中，最重要的表现就是随着科学技术的迅猛发展，个人信息安全处于越来越多的风险与不确定性之中。与其他风险相比，个人信息受损中的风险具有如下特殊性：第一，某些极具识别性的信息如基因信息等一旦泄露即具有不可挽回性，无法通过销毁、重置等手段使此类个人信息恢复到隐秘的状态，因而是一种不可逆的风险；第二，扩散性，以暗网为例，暗网上交易、转卖的个人信息正以极高的频率、极广的范围传播，如据江苏南通和如东公安机关调查，暗网上超过 5000 万份公民个人信息被出售；〔27〕第三，不可测性，一旦个人信息泄露，无法通过追踪、停止侵害等方式使个人信息重归于可控范围。

亦即言，数字时代的自然人，其个人信息泄露后可能以不可知的方式无限次地传播，从而使相应的自然人深受其害。若法律对此置之不理，而是坐等一切风险全部转化为不可逆的损害之后才予以救济，难免过于消极，并不利于法律充分保护民事主体合法权益之目的的实现。事实上，风险社会理论在数字时代复兴，其中蕴含的是一种在不可挽回的悲剧发生之前尝试避免的努力。为此，对于个人信息侵害导致前述风险的法律规制，最有效的途径之一便是将现实损害发生前已存在的特定风险纳入侵权法的调整范畴，通过侵权法上的责任认定与承担机制将最终的不利益转移到信息处理者一方，督促信息处理者提前规避个人信息侵害行为发生，从根源上加大保护个人信息的力度。事实上，通过承认特定风险在侵权法上的可赔性，从而将引发特定风险发生的不利益由受害人转移给信息处理者承受，在侵权法上亦具有充分的正当性基础：第一，个人信息泄露

〔25〕 参见前引〔3〕，叶名怡文。

〔26〕 参见〔德〕乌尔里希·贝克、约翰内斯·威尔姆斯：《自由与资本主义——与著名社会学家乌尔里希·贝克对话》，路国林译，浙江人民出版社 2001 年版，第 119 页。

〔27〕 参见苏锦安、戴红亮：《5000 多万条个人信息在“暗网”倒卖》，载 https://baijiahao.baidu.com/s?id=1666342996935526862&wfr=spider&for=pc，最后访问时间：2022 年 4 月 5 日。

后导致的种种风险均由信息处理者的行为产生，由开启危险源的人承担责任，符合侵权法的基本法理；第二，信息处理者通常比个人具有更强的风险规避能力；第三，信息处理者通过搜集海量个人信息从中获利，根据报偿理论，也应由信息处理者承担个人信息侵害导致的风险。〔28〕

在侵权法上，让加害人对其造成的损害进行赔偿，实质上是将其侵权行为带来的成本内部化，从而迫使行为人的行为符合社会预期，同时也能实现对他人利益的保护。〔29〕在风险社会背景下，对侵权损害赔偿的相关理论进行适时调整，适当地将个人信息侵害引发的特定风险纳入侵权法上的可赔范畴，在现实的损害发生之前即予以调整，既能发挥预防损害发生的作用，实现帕累托最优，又能实现侵权法的震慑作用，从而更好地发挥侵权法本身的保护作用，实现其规范目的。

（二）将风险作为损害的理论分歧及评析

对于前述个人信息侵害引发的特定风险应否纳入我国侵权法上的可赔损害范畴，我国学理上存在较大分歧。持否定说的学者以损害须具有“确定性”为理由，认为个人信息被泄露只会带来未来发生损害的风险，而这种风险本身不具有“确定性”，因此不能被认定为侵权法上的损害。在否定论者看来，赔偿责任只有在个人信息被非法利用导致现实的人身、财产侵害时才会发生。〔30〕

持肯定说的学者则重申了损害概念需要革新这一命题，其立足于数字时代的风险社会这一背景，认为应将满足一定条件的风险认定为侵权法上的损害，这相当于将信息泄露而导致其他现实损害发生的风险由受害人转移给信息处理者承担。在肯定说看来，由信息处理者承担这种风险是风险社会分配风险的一种具体方式。至于风险性损害与损害的“确定性”之间的矛盾并非不可调和，其可以通过对“确定性”作进一步的开放性解释获得解决，而不是自始将“确定性”等同于“已发生”。〔31〕以此为基础，肯定说认为，对于将个人信息侵害引发的特定风险纳入侵权法上可赔偿损害范畴所面临的难题，应从对差额说的修正出发，将侵权行为导致的状态差额作为认定损害存否的标准，〔32〕然后建立起动态的评价体系，按照此标准对个案中发生的风险进行判断，予以灵活确定。〔33〕

在否定说和肯定说之间还存在折中立场。持此立场的学者一方面并未承认将风险本身视为一种损害，另一方面又认为个人信息泄露造成的风险本身也会带来现实的财产减损，在某些情况下会造成严重的精神损害，而这些不利益可以纳入侵权法的损害范畴并得到相应的救济。如受害人为了预防个人信息泄露导致的风险现实化而支出的预防费用，可以被认定为与侵权行为具有因果关系的财产损失。〔34〕此外，考虑到实践中精神损害的严重程度本身难以判断，折中说对个人信息侵害中承受风险的受害人是否存在严重精神损害进行推定。在其看来，只要是严重侵权，那么

〔28〕 参见刘水林：《风险社会大规模损害责任法的范式重构——从侵权赔偿到成本分担》，载《法学研究》2014 年第3 期。
〔29〕 参见前引〔12〕，陈聪富文。
〔30〕 参见程啸：《论大数据时代的个人数据权利》，载《中国社会科学》2018 年第 3 期。
〔31〕 参见前引〔5〕，田野文。
〔32〕 参见前引〔11〕，李昊文。
〔33〕 参见张建文、时诚：《个人信息的新型侵权形态及其救济》，载《法学杂志》2021 年第 4 期。
〔34〕 参见前引〔4〕，谢鸿飞文。

相应的精神损害即可以推定为具有严重性。亦即言，在承认个人信息侵权行为属于“严重侵权行为”的基础上，也应承认这样的侵权行为会导致具有“严重性”的精神损害。因此，个人信息侵权本身也可能会造成财产损失与严重的精神损害从而得到赔偿。〔35〕

从前述学理讨论可知，否定说和折中说均对于个人信息泄露导致的风险本身被认定为损害这一问题持否定态度，只有肯定说承认了个人信息泄露本身产生的风险可能被认定为损害。否定说和折中说对风险作为损害的否认是基于风险不具有确定性这一理由，而肯定说对确定性作出了不同的解释，从而得出一定的风险也可以具有确定性的结论。对此，本文认为，将风险作为损害认定问题上的分歧，根源在于对损害概念理解上的不同。持否定说的学者之所以否认风险作为损害，是基于对差额说的坚持，认为无现实的财产差额则不可能存在财产损失。因而对于损害本质的理解就成为理解这一问题的关键，本文认为，损害概念本身不应狭义地理解为差额，差额说仅为财产损失的一种认定方式，尽管其一直以来占据主流的地位，然而在个人信息侵权领域仍有对其修正适用的必要性。

（三）将风险作为损害的理论基础

如前所述，虽然差额说一直是侵权法上认定财产损失的基础理论，但不能将损害直接等同于差额，差额仅仅是损害的认定方式之一，去价值化的特性导致其在特殊情形下难以认定损害是否发生。以个人信息侵权中的损害为例，受害人除了遭受现实损害之外，还可能遭受个人信息泄露导致的一系列风险，如下游犯罪剧增、社会分选与歧视、消费操纵和关系控制，虽然信息泄露导致的这类风险并不直接体现为现实的财产差额，但是受害人所处的利益状态本身事实上已发生了实质变化，比如身份信息被盗窃后可能导致不良个人信用记录，或者隐私信息被雇主非法获取后变成“透明人”，在就业市场上的竞争力下降，获得雇主青睐的能力降低，等等。在差额说下，受害人这些状态的恶化均难以被认定为侵权法上的损害而获得赔偿，难免有失偏颇。

损害概念的本质是受法律保护的状态或地位遭受不利益，若这些状态的变化已具有相当的确定性，也足以用金钱衡量，那么自然应肯定相应损害的存在。若差额说无力解决这一问题，那么不应缘木求鱼，而是有必要引用学理上对差额说进行修正的其他学说来认定损害。如规范损害说主张，即使并无特定物或人身权益被侵害或者并不存在财产总额之价值变动，只要权利主体受法律保护的地位被侵害或者存在纳入法律规范评价领域的损害，那么这些侵害或者损害就属于侵权法上的可赔损害范畴。学理上存在对规范损害说的批判，认为其只是一种思维方式，难以避免缺乏客观标准导致的司法自由裁量权滥用等问题。〔36〕对此，本文认为，规范损害说虽然不能取代差额说的位置，但在差额说并不能解决的特殊问题上，可以通过引入规范损害说而赋予法官以自由裁量权，从而克服差额说之弊端，更好地服务于法律保护个人信息之目的。事实上，我国司法实践中已有法院采取了这样的观点。例如，在“孙长宝与北京搜狐互联网信息服务有限公司等人格权纠纷案”中，北京市互联网法院认为“个人信息在互联网经济的商业利用下，已呈现出一定的财产价值属性”，并且信息处理者从获取个人信息中获益，因此也应当承担相应风险导致的不

〔35〕 参见前引〔4〕，谢鸿飞文。

〔36〕 参见朱晓峰：《侵权可赔损害类型论》，法律出版社 2017 年版，第 70 页。

利益，对被侵权人的损失和利益没有证据的，应当根据实际情况确定赔偿数额。〔37〕

（四）将风险作为损害的比较法经验及启示

对于风险能否被认定为损害的争论并不仅存在于我国。在比较法上，如美国的司法实践中风险是否应作为侵权法上的损害而可以通过金钱赔偿的方式予以救济，也颇具争议。支持将特定风险作为损害的观点认为，在原告能初步证明未来发生损害的可能性非常高的情况下，应当承认原告有资格以这种风险作为损害起诉，并有资格获得赔偿。在 Remijas v. Neiman Marcus Grp. LLC 案中，法院便在原告并未受欺诈而仅仅存在风险的情形下认定原告遭遇了现实的损害。〔38〕在 Lewert v. P. F. Chang's China Bistro，Inc. 案中，法院更进一步指出，两名被黑客窃取信用卡信息的原告，虽然其中一名已经遭受欺诈而另一名没有，但两名原告都因为得知自己的信用卡信息被泄露而费时费力地监控其账户，因此原告所主张的损害已然发生，〔39〕亦即应将风险出现后受害人为了防范风险而付出的预防费用也认定为损害予以赔偿。与之相反，持否定立场的法院则认为风险本身并不具有实质性、确定性，因此不应纳入可以获得侵权赔偿的损害范畴。在 Clapper v. Amnesty International USA. 案中，原告质疑美国《外国情报监视法》中允许监控境外非美国公民的通信的相关规定，原告认为这增大了自己的隐私或其他个人信息被泄露的风险，不但会使其一直处于不安全的焦虑状态，还会使其为了防止自己的隐私泄露而付出时间和金钱的成本，这已然构成损害。然而这一诉求被美国联邦最高法院拒绝。〔40〕这一案例被很多法院在支持否定说时加以引用。因此，在许多被黑客攻击后个人信息泄露的案件中，法院并不支持仅仅以风险作为损害而起诉的做法，拒绝承认“实质性风险”的说法，比如 Key v. DSW Inc. 案〔41〕与 Beck v. McDonald 案。〔42〕

相比之下，欧盟对个人信息保护力度更大，因而对新型损害的认定也持有与美国法院的否定说不同的态度。欧盟的《通用数据保护条例》即反映了放宽损害要件认定标准的立场，从而加大了个人信息的保护力度，以回应个人信息侵权愈演愈烈背景下保护个人信息权益的现实需求。例如，《通用数据保护条例》第 82 条将可以主张损害赔偿请求的范围扩大到了“遭受重大或非重大损害的人”，放弃了损害具有重大性才可主张赔偿的要求。另外，该条例第 146 条有更为明确地表示：“损害应根据欧盟法院的判例法作广义解释，并充分反映本条例的目标。”此条直接地为个人信息侵权所可能带来的社会分选与歧视、精神损害等被纳入新型损害的范畴，提供了可能性。

为追随欧盟《通用数据保护条例》保护个人信息的规范目的，德国法也降低了损害认定门槛，缓和了对“实际金钱损害”“精神损害之严重性”等要件的强调，以加大对个人信息的保护力度。这具体表现在两个方面：一是就风险本身是否具有经济价值、受害人是否可以因此主张赔偿而言，德国开始将“歧视、身份盗窃或欺诈、财务损失、声誉损害、数据泄露”等不利益纳入

〔37〕 参见北京互联网法院（2019）京 0491 民初 10989 号民事判决书。

〔38〕 See Remijas v. Neiman Marcus Grp. LLC，794 F. 3d 688（7th Cir. 2015）.

〔39〕 See Lewert v. P. F. Chang's China Bistro，Inc，819 F. 3d 963（7th Cir. 2016）.

〔40〕 参见前引〔2〕，Kristen Choi 文，第 444 页。

〔41〕 See Key v. DSW Inc，454 F. Supp. 2d 684（S. D. Ohio 2006）.

〔42〕 See Beck v. McDonald，848 F. 3d 262（4th Cir. 2017）.

损害的行列，并承认此类不利益可能带来财产损失；二是就风险是否会导致精神损害而可主张精神损害赔偿而言，2018 年新修订的《德国数据保护法》已经将精神损害索赔门槛明显降低，删除了原本的“严重侵害人格权”这一要件。〔43〕

当然，各国对个人信息的保护力度存在明显差异，因为对个人信息采取何种保护本身就属于价值判断的问题。个人信息除了承载着个人受法律保护的利益之外，同时也承载着公共利益。一些学者甚至提出，个人信息对当代经济的重要性就像石油对工业革命的重要性一样。〔44〕将个人信息加以合理利用、整合，已经成为提高政府治理水平、提高生产力发展速度和质量必不可少的要素之一。因此，在个人信息权人的合法利益与社会公共利益保护的天平上，立法者如何进行价值取舍与权衡，将直接决定法律实践对个人信息的保护力度。典型的弱保护模式是美国模式，它几乎不保护一般的非隐私信息。〔45〕与此相对应，美国法院对于风险作为损害的态度以否定说为主即不足为奇。相比之下，欧盟及其成员国对个人信息的保护明显更强。因此，在借鉴域外经验时也应将此背景纳入考虑，结合我国立法对个人信息保护的态度进行取舍、有选择性地借鉴相应的有益经验。本文认为：一方面，我们不能不考虑个人信息侵权愈演愈烈、受害人主张侵权法上的损害赔偿却极难得到支持的司法现状，以及比较法上放宽损害要件、降低证明难度等以达到加强个人信息保护力度的趋势；另一方面，又不能在风险作为损害这一问题上捕风捉影，一概支持将风险认定为损害，以此造成对个人信息的过度保护进而抑制利用个人信息所内含的公共利益的保护。因此，对于哪些风险能被认定为侵权法上的损害予以赔偿这一问题不能采取“全有全无”的判断策略，而应该建立动态评价体系，在个案中结合规范目的具体判断，被予以承认的风险性损害应是客观的、合理的，而非主观臆测的、捕风捉影的。

四、个人信息侵权中的损害认定方法

个人信息侵权案件中的损害认定相较其他侵权案件更为复杂。一是损害的类型更为复杂；二是损害可能发生在收集信息、处理信息、散布信息以及后续传播等各个环节，可能发生二次损害甚至多次损害。本文认为，发生个人信息泄露或其他个人信息侵权事件时，受害人可以主张的损害可以区分为现实损害与风险性损害。现实损害又可以进一步区分为财产损失和精神损害，至于风险性损害，法官需在个案中分别进行利益衡量，满足一定条件的风险性损害应纳入侵权法上的损害范畴而获得相应的赔偿。

（一）财产损失

个人信息侵权导致的财产损失按照其产生原因不同，可大致分为三类：其一，个人信息权益作为可被商业化利用的人格权益，其本身具有财产利益的属性，在个人信息权益被侵害时，权利

〔43〕 参见前引〔3〕，叶名怡文。

〔44〕 See Sam Jossen，The World's Most Valuable Resource is No Longer Oil，But Data，*The Economist*，May 6，2017.

〔45〕 See Shawn A. Johnson，A Law and Economics Approach to Privacy Policy Misstatements：Considering the Need for a Cost Benefits Analysis in the FTC's Deception Framework，18（1）*Columbia Science and Technology Law Review* 79，79－138（2016）.

主体可主张对个人信息所具有的财产价值减损的赔偿；其二，侵权行为人在侵害个人信息权益的同时，很可能导致其他财产权益受损；其三，个人权益受到侵害时可能导致各类风险，受害人为了防范这类风险的现实化可能付出风险防范费用，这在一定条件下也可能成为受害人可主张的财产损失。

1. 个人信息权益本身的财产价值损失

尽管我国民法学界对个人信息权益属于权利抑或利益存在分歧，但这并不影响主流观点在个人信息属于独立的人格权益这一问题上达成共识。〔46〕即自然人享有的个人信息权益可归入《民法典》第990条第2款规定的人格权益范畴。

个人信息权益作为一种独立的人格权益不仅仅承载着权利主体的精神利益，还承载着经济利益。〔47〕比如权利主体通过将个人信息授权于他人使用或转让给他人进行商业化利用，实现对其个人信息权益的经济利益。当个人信息权益受侵害时，其本身的财产价值可能发生减损因而产生财产损失，这种财产损失是因个人信息权益作为一种人身权益被侵害而导致的，有别于财产权益直接受损而导致的财产损失。我国的法律实践坚持人格权一元保护模式，当受害人基于其人格权受损害而受到财产损失或精神损害时，无需分别主张财产利益和人格权利益受到侵害而获得赔偿，而是通过人格权制度对财产、精神利益同时予以保护。〔48〕《民法典》第1182条中规定，侵害人身权益造成财产损失的，赔偿数额的确定可以根据实际损害、侵权人获益确定，或者由法院酌定，这一规定也是为了适应人格权益受侵害导致财产损失的情形，即人格权益本身受损时也可直接主张财产损失。将财产性的考虑引入人格权的损害纠纷中，其目的是突破人格权损害以精神损害赔偿为主的藩篱，为权利人提供更为全面的权利救济。〔49〕

2. 下游财产损失

个人信息被信息处理者收集后，可能被第三人窃取或利用，第三人利用个人信息进一步实施侵权行为，最常见的有窃取个人信息实施诈骗或盗窃，此类情形下，受害人直接遭受财产损失，因而对侵权责任损害要件的认定并无太大争议。理论和司法实践中的争议主要集中在信息泄露造成的财产损失结果是否应当由信息收集平台承担、在多大程度上应当由其承担责任，以及不同责任人之间如何分担侵权损害赔偿责任。〔50〕至于财产损失的数额认定，可直接采差额说的界定标准，计算侵权行为发生后的实际情况与假设侵权行为未发生的应然情况之间的财产差额，以此作为赔偿金额。

3. 风险的预防费用

个人信息被信息处理者泄露后却并未被第三人立即进一步利用实施侵权行为，在这种情形下，虽然受害人财产并未发生现实的减少，但是由于其个人信息已经处于随时可能为第三人非法利用的状态，可能引发下游犯罪、社会分选和歧视、消费操纵和关系控制等等。这些情形均不能

〔46〕 参见张新宝：《论个人信息权益的构造》，载《中外法学》2021年第5期；彭诚信：《论个人信息的双重法律属性》，载《清华法学》2021年第6期；付新华：《个人信息权的权利证成》，载《法制与社会发展》2021年第5期。

〔47〕 参见向秦、高富平：《论个人信息权益的财产属性》，载《南京社会科学》2022年第2期。

〔48〕 参见程啸：《论我国民法典中个人信息权益的性质》，载《政治与法律》2020年第8期。

〔49〕 参见姚辉：《关于人格权商业化利用的若干问题》，载《法学论坛》2011年第6期。

〔50〕 参见谢鸿飞：《个人信息处理者对信息侵权下游损害的侵权责任》，载《法律适用》2022年第1期。

直接认定为受害人财产状况现实的削减，而仅仅是未来可能产生财产损失或其他不利益的风险。受害人可能为了防止前述风险的实现，不得不采取一定措施将自己的状况保持在风险不会发生的状况。比如被黑客攻击电脑系统后，为防范数据为第三人不法利用而安装防火墙或更换系统并自费安装防护软件；又比如信用卡信息被非法盗取后挂失信用卡等措施均会带来一定的金钱成本，这些费用虽然区别于一般意义上的财产损失，但其支出目的在于防范第三人非法利用已泄露的个人信息对其权益造成侵害、避免将来可能的损害风险，是为了排除对权益的妨害，〔51〕与加害人侵害个人信息的行为之间具有因果关系，可以认定为损害而获得赔偿。

此外，个人信息侵权的司法解释也明确规定，为防止人身伤害的发生而采取的某些必要措施的合理费用也构成财产损失。〔52〕虽然司法解释中仅仅列举了律师费、调查取证的成本作为排除人身权益妨害的预防费用，可以作为损害而获得赔偿，但不排除其他的预防费用也可以通过类推解释的方法获得赔偿的可能性。

至于赔偿数额的问题，并非任何预防费用均可获得全额的赔偿，比如在美国 Polanco v. Omnicell，Inc. 案中，预防费用的可赔性受到严格的限制，在不存在法律上的因果关系的情形下，或者预防费用并非合理必要而仅仅是受害人故意“制造”的情形下，预防费用不可认定为损害而获得赔偿。〔53〕因此，在划定预防费用的可赔范围时，本文认为可以在比例原则下审视：此项预防费用的支出是否具有合理性、必要性和相称性，仅仅在合理范围内符合比例原则的预防费用可以获赔，以此防范受害人通过恶意“制造”预防费用引发的道德风险事件，以维护“禁止从损害中获益”这一法理。

（二）精神损害

根据《民法典》1183 条第 1 款，受害人因人身权益被侵害而遭受的精神损害只有满足“严重性”要件时才可获得赔偿。在司法实践中，因个人信息泄露导致的精神损害往往因为达不到“严重性”要件而难以获得法官支持，比如“黄某诉腾讯科技（深圳）有限公司等隐私权、个人信息权益网络侵权责任纠纷案”中，受害人因其个人信息被泄露而主张精神赔偿，但却由于泄露的范围限于其微信好友，故原告主张的精神损害因达不到“严重性”标准而不被支持。〔54〕

事实上，精神损害是否满足“严重性”要件这一问题并不单单是在个人信息侵权中特有的问题，而是所有主张精神损害赔偿的案件中固有的问题，由于“严重”一词固有的模糊性和空洞性，学理上对其的认定标准缺乏共识甚至相互矛盾，导致无法对司法裁判起到有效的指导作用。因此，在司法实践中，法官往往滥用自由裁量权，难以对类似案件实现类似处理。〔55〕实际上，“严重性”作为法律条文中的表述，对其解释应该成为评价社会事实的一种应然价值标准，“精神损害是否具有严重性”这一问题绝非仅仅是事实的判断，更是根据社会一般观念、立法者的规范目的而进行一系列价值衡量的结果。

---

〔51〕 参见前引〔8〕，程啸书，第 170 页。

〔52〕 参见《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》第 18 条；《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》第 8 条。

〔53〕 See Polanco v. Omnicell Inc，988 F. Supp. 2d 451，470－71（D. N. J. 2013）.

〔54〕 参见北京互联网法院（2019）京 0491 民初 16142 号民事判决书。

〔55〕 参见朱震：《论侵害人格权精神损害赔偿中的“严重”》，载《法制与社会发展》2022 年第 2 期。

因此，在个人信息侵权中受害者主张的精神损害是否具有“严重性”，也有赖于法官在个案中综合考量各种涉案因素的基础上进行价值衡量来确定。针对受害人因个人信息泄露导致的风险而产生的“焦虑”这一情形，首先，法官应该考虑社会中风险分配的问题，即哪些风险应该由处理者承担，哪些精神负担和心理压力应该由受害人自己负责。其次，法官也应该视被侵害的个人信息属于私密信息抑或非私密信息区分不同的保护力度，比如在隐私权受到侵害时，相比一般的个人信息被泄露的情形，受害人正常的生活安宁、平静和不受侵扰的状态往往受到更大的冲击，此时其主张的精神痛苦严重程度也就更高。最后，受害人主张的精神损害可能是基于个人信息受损，也可能是基于其他人格权益受损，比如因个人信息泄露导致的名誉权受损而产生的精神损害。《民法典》对于不同人身权益类型进行区分保护，这也会影响精神损害“严重性”要件的判定。《民法典》第 998 条中将生命权、身体权、健康权区别于其他人格权，可见其作为自然人赖以生存的基本人格权地位，因此对其保护程度也应相应最高。〔56〕对于第 998 条生命权、身体权、健康权之外的精神性人格权，立法者持有开放的态度而将相应的利益衡量授权给法官，在判断侵害精神性人格权的民事责任时，法官可以根据第 998 条中列举的因素自由裁量，这当然也适用于精神损害的“严重性”要件的判断。〔57〕

（三）风险性损害

根据规范损害理论，损害的认定应以“受害人受法律保护的状态或地位是否发生变动”作为标准。就个人信息领域的损害认定而言，个人信息泄露带来的风险状态与零风险或低风险状态相比较，是否存在客观真实的利益差额？这种利益差额在立法者的价值立场上，究竟是由受害人自己承担还是由信息处理者承担？对此，法官在个案中应该围绕状态差额进行价值衡量，具体判断哪些风险可被认定为损害。为了约束法官的自由裁量权，法官在进行价值衡量时应在如下考虑因素框架下进行动态评价。

1. 被侵害的个人信息类型

法官在进行利益衡量时，应首先考虑我国现行法律框架下立法者所持的价值立场以及追求的规范目的，损害的认定也应与现行法的规范目的和秩序相匹配。根据《民法典》第 1032 条第 2 款和第 1034 条第 3 款，个人信息中的私密信息属于隐私范畴，侵害私密信息后应优先适用关于隐私权的保护规定，这表明立法者对于私密个人信息和一般个人信息事实上进行区别保护。在侵犯隐私的情况下，由于损害的范围已经扩展到无形损害，侵犯私密信息本身即可以认定为损害。〔58〕《民法典》第 1226 条对此即作了明确规定。依据该条规定，医疗机构及其医务人员对披露患者病历承担侵权责任，该条隐去了损害要件，事实上表明立法者承认于此情形下私密信息披露本身就可以构成损害，而无需其他现实的损害结果。〔59〕在司法判决中，法官也持对隐私权进行绝对保护的立场，隐私权本身的侵害即可被认定为损害。〔60〕

〔56〕 参见黄薇主编：《中华人民共和国民法典人格权编解读》，中国法制出版社 2020 年版，第 47 页。

〔57〕 参见前引〔55〕，朱震文。

〔58〕 参见徐明：《大数据时代的隐私危机及其侵权法应对》，载《中国法学》2017 年第 1 期。

〔59〕 参见前引〔5〕，田野文。

〔60〕 参见贵州省贵阳市中级人民法院（2021）黔 01 民终 975 号民事判决书；北京市房山区人民法院（2020）京 0111 民初 12513 号民事判决书。

因此，如果被泄露的信息是私密信息，则可以适用对隐私权进行绝对保护的规定，无论这种信息泄露是否导致现实的财产损失或精神损害，无论会导致何种风险，这种泄露本身都可以直接被认定为损害，而不再需要法官对风险展开进一步的考察。然而，个人信息应因其私密程度差异而受到不同程度的保护，否则难免会抑制个人信息被传播、利用创造的社会价值。因此除了私密信息以外的个人信息被泄露导致的风险，需要进一步讨论是否构成损害。

2. 风险发生的盖然性

在私密信息以外的个人信息被泄露的情形下，各类风险需要进一步予以考察以认定是否能构成损害。对此，风险的界定有两个精细化方向：一方面，它包含了特定危害后果发生的可能性，即概率；另一方面，它包含了危害的结果及其影响的范围。〔61〕美国联邦最高法院在 Spokeo, Inc. v. Robins 案中指出，满足一定盖然性条件的无形风险也能被认定为确定、具体的损害。〔62〕只有具有较高盖然性的风险才会给受害人带来现实而紧迫的威胁，如不及时制止和排除，则很可能带来不可逆转的后果，因而有必要认定为损害并予以救济。有学者将不同盖然性的风险分为三类，即“危险”“风险”和“剩余风险”。〔63〕其中，“危险”的盖然性最高，社会一般人通过直观经验即可感受到权益受到侵害的威胁；“风险”的盖然性相较更低，但仍然在客观上对受害人带来威胁，与剩余风险的“几乎不可能发生”的状态相比，“风险”仍有救济的必要。对于什么样的风险值得保护，有不同的观点。有观点认为，应该证明伤害几乎肯定会发生，只有在因果关系不能充分证明的情况下才能预防；还有观点认为，只要有伤害发生的可能性，这种风险就应该提前预防。〔64〕尽管存在分歧，但这两种观点均认为：“风险”要求的证据充分程度应低于采取危险排除行为的证据要求，也即除了“危险”可以通过消除危险请求权加以救济之外，给受害人带来损害的盖然性达到一定标准的“风险”也可以认定为损害，受害人有权主张恢复原状或赔偿予以救济。〔65〕

判断个人信息泄露导致的风险发生的盖然性，可以结合以下几点具体判断：

第一，信息泄露的范围是否足够广泛。在通过网络侵害个人信息时，可以根据点击率、转载率、持续时间、传播范围等因素来评估影响范围。〔66〕如果个人信息在披露后的传播仍在可预见和可控范围内，不属于向不明人群或不明地区的传播，则风险转化为实际损害的可能性一般较小。〔67〕反之，如果影响范围足够大，则受害人受法律保护的财产、人身安全状况则会发生实质的变化，风险发生的盖然性则更大。

第二，结合信息出于何种目的被收集，又以何种方式被泄露、窃取等相关因素考察。从行为

〔61〕 参见赵鹏：《风险社会的行政法回应：以健康、环境风险规制为中心》，中国政法大学出版社 2018 年版，第 10 页。

〔62〕 See Daniel J. Solove, Danielle Keats Citron, Risk and Anxiety: A Theory of Data Breach Harms (December 14, 2016), GWU Law School Public Law Research Paper No. 2017 - 2, GWU Legal Studies Resarch Paper No. 2017 - 2, p. 1244.

〔63〕 参见秦天宝、陆阳：《从损害预防到风险应对：预防性环境公益诉讼的适用基准和发展方向》，载《法律适用》2022 年第 3 期。

〔64〕 1987 年保护北海第二次会议部长级宣言指出：为保护北海免受危险物质损害的可能，采用预防措施十分有必要，要求在损害因果关系得到充分科学证据确认之前控制危险物质的注入。

〔65〕 参见前引〔61〕，赵鹏文。

〔66〕 参见前引〔33〕，张建文、时诚文。

〔67〕 参见“张某某等与俞某等隐私权纠纷上诉案”，浙江省杭州市中级人民法院（2017）浙 01 民终 3053 号民事判决书。

目的来看，第三人出于黑客攻击的目的获取个人信息，和商家出于精准投放广告、营销的目的非法获取个人信息相比，显然前者的行为利用个人信息从事违法犯罪的可能性更大。从行为方式来看，如果第三人仅仅是盗窃有形财产比如电脑、手机等，行为人在将有形财产据为己有的同时，很可能通过解锁而获知手机里和电脑里的相关个人信息，但是这种非法获取个人信息的方式和黑客直接精准攻击大量的网络用户系统、定向获取特定数据相比，显然后者更具有直接的攻击性和危害性，其所引发的风险转化为现实损害的可能性更大。

第三，在诉讼程序中，受害人也可以在举证中通过类似的信息泄露事件中风险是否发生来证明风险的盖然性。例如，“庞理鹏与北京趣拿信息技术有限公司等隐私权纠纷案”中，原告收到虚假的航班信息取消短信，其通过列举出东航公司多次被媒体曝光存在泄露他人个人信息的风险先例，〔68〕加之近年来航班信息的诈骗事件多发的社会背景，以此证明自己个人信息被盗窃后被诈骗之风险的盖然性，该主张最终被法院采纳。通过列举类案中风险发生之盖然性之高，可以对受害人所遭受的风险发生之盖然性起到佐证的作用，因此也可以作为法院在认定风险性损害时的考量因素。

3. 风险可能导致的危害及其影响范围

正如上文所言，风险的另一个精细化方向为风险可能导致的危害及其影响范围，只有对于可能引发不可逆转的重大损失的风险才有必要提前采取预防措施。风险之所以有被认定为损害的必要性，也是基于个人信息领域某些信息泄露导致的风险将产生不可逆转的损害，而不得不提前采取预防措施。在环境法领域，《里约环境与发展宣言》第 15 条明确指出，那些严重的或者不可逆转损害的威胁属于需预防的风险。〔69〕这一规定对于哪些风险是值得预防的判断标准来说具有借鉴意义。因此，本文认为，要认定为损害的风险应首先满足损害后果不可补救或者事后补救将带来巨大的成本这一条件，否则将损害与赔偿的认定提前到实际损害发生之前便失去其必要性。就不能补救而言，如某些个人信息一旦泄露便难以通过更改个人信息的方式消除被泄露的风险，如生物识别信息或者基因信息，如果对于这些风险都采取一定的预防措施，即提前认定为损害而予以赔偿，那么便可消除信息处理者的侥幸心理，督促收集、保管生物基因信息的处理者更加谨慎行事，以免发生不可逆转的后果，从而发挥损害赔偿的预防作用。就补救所需成本巨大而言，被泄露的个人信息在“暗网”被倒卖后，无数下游处理者将随时都可以反复利用这些个人信息实施不法侵害活动，使可能的损害将在未来不定期地反复发生。受害人若是等到具体的损害结果发生后才能主张赔偿，将不得不在长期的不确定性状态中等待数月甚至数年才能得到救济，受害人为维权付出的时间成本和金钱成本也会随之增多。

五、结　论

整体而言，在数字时代，通过重新审视损害概念而在引入规范损害说修正差额说之不足的基

〔68〕 参见北京市第一中级人民法院（2017）京 01 民终 509 号民事判决书。

〔69〕《里约环境与发展宣言》第 15 条规定：“为了保护环境，各国应该根据它们的能力广泛采取预防性措施。凡有可能造成严重的或不可挽回的损害的地方，不能把缺乏充分的科学肯定性作为推迟采取防止环境退化的费用低廉的措施的理由。”

础上，可以将特定条件下个人信息侵害引发的风险纳入侵权法上的可赔损害范畴，从而更好地落实法律充分保护自然人合法权益的目的。至于哪些风险可被认定为损害，应着重考虑的方向是：其一，我国现行法对私密信息和其他个人信息实行区别保护，因此在认定特定风险可否作为损害时，应区分个人信息私密程度不同而有所差异；其二，对于非私密信息的侵害，应从风险发生的盖然性和风险可能导致危害的影响范围两个维度考察风险是否具有被认定为损害的特质。法官在认定风险性损害和确定损害数额时，应在个案中综合以上考量因素进行利益衡量、动态评价。

Abstract: In view of the irreversibility, unpredictability and proliferation of certain risks in the context of modern society, identifying risks as legal damages before irreversible consequences occur and obtaining compensation through tort law can internalize the costs of tort, which can play a preventive role to achieve Pareto optimality and also achieve the deterrent effect of tort law. Therefore, in the case of personal information infringement, in addition to the actual damages such as property damages and moral damages, the risky damages that meet certain conditions should also be recognized as legally compensable damages. In the determination of risky damages, the normative damage theory should be used as the theoretical basis for the determination of damages, and a dynamic evaluation system should be established to determine the amount of damages based on specific considerations in individual cases.

Key Words: personal information infringement, differential theory, normative damage theory, risk society, risky damage

（责任编辑：徐建刚　赵建蕊）

财经法学 No. 5，2022
pp. 95 - 106

个人信息私法救济中的“损害赔偿”困境与应对路径

赵贝贝 *

内容提要：作为救济个人信息权益损害的民事责任之一，损害赔偿责任在侵权责任承担方式体系中具有核心地位。然而，实证数据和案例分析表明，司法实践对侵害个人信息损害赔偿责任的适用多持严苛态度，其中损害的认定已成为其中的首要障碍。从风险规制理论的视角来看，将信息风险性损害纳入法律上的损害范畴是一种高效的风险分配路径，更是化解私法保护困境的有效出路。此外，为确保信息侵权损害赔偿责任的落实，应凭借“差额说”将信息风险性损害具体化为附带财产损失和焦虑引起的精神损害等样态；适当缓和精神损害的严重程度要求；明确财产损失、精神损害、惩罚性赔偿的赔偿数额之计算规则，以更好地发挥损害赔偿填补损失的功能。

关键词：个人信息权益　风险性损害　损害赔偿规则　惩罚性赔偿

一、问题的提出

我国公法对个人信息权益保护的立法回应虽早于私法，但因刑事责任或行政责任的着眼点在于向国家承担责任，对私权利的救济仍需仰赖具有财产性质的民事责任。正因如此，《个人信息保护法》第 69 条第 1 款规定：“处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。”这使得损害赔偿成为信息侵权民事责任的“代名词”。但在个人信息侵权领域，单纯侵害个人信息极少伴随着信息主体财产、身体实际

* 赵贝贝，武汉大学法学院博士研究生。

本文为教育部人文社会科学研究规划基金项目“民法典制定背景下程序法与实体法融合机制研究”（17YJA820017）的阶段性成果。

受损等直接物质性损害，通常带来的是风险或焦虑不安等非物质性损害。对此，信息主体主张的损害类型较为多元：一是实际发生了诈骗等侵权行为并造成现实经济或精神损害；二是个人信息的孤立经济价值减损；三是个人信息泄露带来的未来损害风险及内心焦虑不安；四是因信息侵权行为而增加的预防风险费、诉讼费、交通费等附带财产支出。然而，由于外部风险或内心焦虑等损害难以被传统侵权法损害概念所接纳，法院常以信息主体无法证明其已遭受实质性损害或无法律依据为由否定第三、四种情形下的损害。在个人信息被过度收集、滥用等侵权行为不断见诸报端、而人的行为风险又无法根除的现代社会，为使处于风险中心的信息主体获得司法的有效救济，我们必须反思：信息主体可主张的损害是否应当包括外部风险或内心焦虑；若包括，需满足的条件要求是什么以及如何凭借“差额说”将风险性损害予以具体化；在信息损害确定后，又如何使事实上的损害真正转变为可获合理赔偿数额的法律上的损害。上述问题正是社会生活高度信息化带来的挑战，而及时应对这些挑战对积累裁判经验和消除实务分歧不无益处。

二、实务视角下的个人信息损害赔偿责任

损害赔偿是侵权法的核心功能，《民法典》侵权责任编将原《侵权责任法》第二章“责任构成和责任方式”修改为“损害赔偿”，进一步明确了以损害赔偿为中心的侵权责任承担方式体系。〔1〕为系统展现个人信息保护的损害赔偿责任现状，本部分以《民法典》施行后的个人信息保护纠纷案件作为分析样本，又虑及规范层面隐私权与个人信息权益在适用规则与案由上存在交叉之现实，笔者分别以“个人信息保护纠纷”“隐私权、个人信息保护纠纷”为案由在“聚法案例网”中做民事案件的检索，共获得裁判文书 359 份（截至 2022 年 2 月 8 日）。在排除撤诉、重复等无效样本的基础上，可将有效个人信息保护纠纷裁判文书进一步限缩为 176 份，围绕主要民事责任方式及审理程序而展开的实证统计结果如表 1、表 2：

表 1　　主要民事责任方式

	停止侵害	赔礼道歉	财产损失赔偿	精神损害赔偿
诉讼请求（份）	103	115	86	106
裁判支持率	82.52％（85/103）	75.65％（87/115）	40.69％（35/86）	26.41％（28/106）

如表 1 所示，信息主体寻求法律救济时，其所主张的停止侵害、赔礼道歉等非赔偿性民事责任诉求一般可通过诉讼程序实现，但对于财产损失赔偿和精神损害赔偿而言，司法实践多持严苛态度。其中法院对精神损害赔偿的裁判支持率仅为 26.41％，呈现出信息主体对损害赔偿的急需与人民法院的微量供给之间的紧张关系。如表 2 所示，损害赔偿责任不仅成为一审和二审争论的问题，连再审率都达到了 4.79％。这在一定程度上说明实务对个人信息损害赔偿责任的认定争议较大，进一步说明以个案为切入点立体剖析赔偿性民事责任之价值。

〔1〕 参见王利明：《我国〈民法典〉侵权责任编损害赔偿制度的亮点——以损害赔偿为中心的侵权责任形式》，载《政法论丛》2021 年第 5 期。

表 2　　审理程序

	一审	二审	再审
损害赔偿诉求（份）	102	37	7
占比	69.80%	25.41%	4.79%

微观视之，司法实务中的个人信息损害赔偿责任主要有以下几方面的问题需要解决：

（一）信息泄露等侵权行为本身是否造成财产损失认定不一

个人信息受侵害时可能会导致或促成下游侵害的发生，并产生相应的财产损失，如不法分子利用被泄露的个人信息实施金融诈骗、伪造证件等行为，〔2〕当引发明显财产性损失时，信息主体主张财产损失赔偿自不待言。问题在于，若下游侵害未现实发生，信息泄露或滥用等侵权行为本身是否造成财产损失呢？侵权法以填补损害为主要目的，若无损害则无填补之必要，〔3〕个人信息权益侵权领域也莫能外。实务中，针对信息被侵害而未造成现实的人身或财产损失时，信息主体主张的财产损失类型通常有两类，即个人信息自身经济价值减损和财产权益未来被侵害的风险。

就个人信息自身的经济价值而言，其以企业数据为表征后无疑蕴含经济利益，部分法院也对此予以了认可。〔4〕但孤立个人数据的经济价值并不高，据相关计算，单个普通人贡献的数据价值为 0.007 美元，而经常出差的富人价值为 1.78 美元。〔5〕在“俞某诉北京乐某达康科技有限公司等网络侵权责任纠纷案”〔6〕中，当事人也仅是根据个人信息的经济价值象征意义的主张 1 元或 2 元赔偿。因个人信息侵权呈现出损害轻微的特点，实务中也并无多少人花费一审、二审甚至再审的高额诉讼成本去追求几元赔偿，法院也常忽视个人信息本身的经济价值。事实上，个人信息的非法交易有着庞大的买家需求，信息泄露的源头行为容易成为其他网络犯罪的“抓手”，因此，人们对于信息泄露等侵权行为的恐惧不在于个人信息自身的价值，而是担忧下游侵害发生的可能性，亦即侵害风险增加或某种机会丧失等。诚然，相对于财产损失或人身伤害易于评估、量化而言，风险多少显得不那么真实。也正是风险与损害确定性标准之间的鸿沟，使得风险能否被损害概念所容并具有赔偿性面临着实践中的挑战。在“孙国燕与被告移动滨州分公司、山东移动公司隐私权、个人信息保护纠纷案”〔7〕中，法院认为被告的电话推销行为直接侵犯了信息主体的知情权与拒绝处理权等信息权利，但对信息主体以未来损害风险为由所主张的财产损失赔偿请求未予支持。而在“孙某某诉沈阳某某家居有限公司隐私权纠纷案”〔8〕中，法院虽然认为被告将个人信息发送到微信群中的侵权行为未造成现实财产损失，但仍认可了信息泄露行为本身造成了财产损失而酌定赔偿 800 元。在个人信息侵权领域，不乏因信息受到侵害而积极维权的当事人，而司法实践对未来风险是否属于侵权损害问题并未形成统一的认识，这无疑将对个人信息的

〔2〕 参见商希雪：《侵害公民个人信息民事归责路径的类型化分析——以信息安全与信息权利的“二分法”规范体系为视角》，载《法学论坛》2021 年第 4 期。

〔3〕 参见王泽鉴：《侵权行为》，北京大学出版社 2009 年版，第 175－176 页。

〔4〕 参见广东省深圳市中级人民法院（2019）粤 03 民终字第 20512 号民事判决书。

〔5〕 参见申卫星：《论数据用益权》，载《中国社会科学》2020 年第 11 期。

〔6〕 参见北京市海淀区人民法院（2018）京 0108 民初字第 13661 号民事判决书。

〔7〕 参见山东省滨州市滨城区人民法院（2021）鲁 1602 民初字第 83 号民事判决书。

〔8〕 参见沈阳市大东区人民法院（2020）辽 0104 民初字第 6814 号民事判决书。

私法保护实践产生消极影响。

（二）附带财产损失是否属于“合理费用”存在理解分歧

发生个人信息侵权行为后，信息主体在个人信息本身损害之外，还存在因利用国家审判制度以实现救济而产生的一些无法避免的律师费、打印费、误工费、交通费等维权成本，以及为避免身份盗用或欺诈风险升高而采取的预防风险支出，上述费用可被统称为附带财产损失，那么信息主体能够以此费用支出诉请赔偿吗？针对侵权损害赔偿范围的划定，我国《民法典》采纳了合理性标准，〔9〕在第 1179 条和第 1181 条第 2 款列举了交通费、误工费等法定赔偿项目，并以“合理费用”作为判断其他损害项目是否属于“等”范围之内的标准。《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》（以下简称《网络侵权司法解释》）第 12 条第 1 款也明确将被侵权人为制止侵权行为所支付的调查费用以及律师费用视为合理费用。由此可见，预防风险支出、部分维权成本等附带财产损失并不属于现行规范明确列举的法定赔偿项目，那么，是否可以归入具有经济赔偿性的“合理费用”范围呢？对此，司法实践中也存在不同的认识。在“戴森、李玉梅与敖馨月隐私权纠纷案”〔10〕中法院认为，原告为维护合法权益委托其丈夫出庭参加诉讼，必然会产生误工损失，因此对其主张的误工费（法定赔偿项目）予以支持。而在“黄茂安与中国移动宜黄县分公司、中国移动抚州分公司等个人信息保护纠纷案”〔11〕中，对原告主张的打印费、交通费、咨询律师费，法院均以没有法律依据为由不予支持。就该案而言，法官在未对交通费、律师费等法定明确赔偿项目予以支持的情况下，反而对并非法定明确赔偿项目的鉴定费予以支持，令人费解。在司法实践中，诸如此类的问题并不在少数，且因为孤立个人信息本身的经济价值微小，受害人主张财产损失赔偿的主要依据又通常是附带财产损失，所以，明确附带财产损失的性质以遏制脱离合理性的裁判分歧现象，是个人信息侵权裁判中无法绕开的话题。

（三）精神损害赔偿认定艰难

个人信息损害通常具有无形性，法院常以信息主体无法证明其已遭受实质损害为由，不支持其财产损失赔偿主张，这几乎挫败了所有基于未来侵害风险提出的财产损失赔偿请求，信息主体对信息侵权损害的救济也转而寄希望于被纳入精神损害赔偿。从个人信息的类型视之，私密信息具有隐私权与个人信息的双重特点。当个人私密信息因被泄露而直接或间接导致明显侵犯隐私权的侵害时，信息主体常通过隐私权保护逻辑主张精神损害赔偿。但在个人信息侵权案件中，精神损害赔偿的支持率仅为 26.41%，而焦虑不安难以被认定为精神损害的子类型，是个人信息精神损害赔偿认定艰难的原因之一。由于个人信息具有数据属性，在个人信息被恶意电子化存储后，不法分子可能会永久获得个人信息数据，受害者因担忧未来被侵害也可能一直处于焦虑不安的精神状态中，〔12〕此种焦虑不安能否被解释为精神损害的子类型呢？与众多裁判文书否定未来风险

〔9〕 参见王磊：《侵权损害赔偿范围的确定机制》，载《法学》2021 年第 4 期。

〔10〕 参见四川省攀枝花市仁和区人民法院（2021）川 0411 民初字第 717 号民事判决书。

〔11〕 参见江西省宜黄县人民法院（2021）赣 1026 民初字第 422 号民事判决书。

〔12〕 See Justin Dion & Nicholas M. Smith, Consumer Protection—Exploring Private Causes of Action for Victims of Data Breaches, 41 *Western New England Law Review* 253, 260 (2019).

性焦虑具有损害赔偿性相反，在“刘云超与被告北京顺丰速运有限公司，第三人严颜个人信息保护纠纷案”〔13〕中，法院不仅支持了原告的赔礼道歉请求，还将原告因个人信息失控产生的可能被用于违法事宜的焦虑不安情绪认定为损害，并部分支持了其主张的精神损害抚慰金。尽管在该案中法院认可了内心焦虑成立损害，但总体而言，法院在审判实践中对内心焦虑的认定持谨慎态度。

此外，即使此类内心焦虑能纳入精神损害的范畴，其也受《民法典》第1183条第1款规定的“严重”要件限制。实践中，法院在大量案件中以损害未达到严重程度为由，拒绝支持信息主体主张的精神损害诉求。例如，在“蔡小燕与赵延安隐私权、个人信息保护纠纷案”〔14〕中，被告未经原告同意将原告及其两子的户籍信息张贴在公开场合，法院支持了原告公开赔礼道歉的请求，但以精神损害未构成严重为由驳回了原告主张仅1元的精神损害赔偿请求。甚至在部分信息主体因个人信息泄露而导致被原公司解雇或遭遇诈骗等行为时，法院仍然认为其精神痛苦不够严重。〔15〕由此可见，法院在审判实践中是普遍默认赔礼道歉责任轻于精神损害赔偿的，即使该精神损害赔偿额为1元也倾向于作出赔礼道歉等非赔偿性民事责任，信息主体若想获得精神损害赔偿绝非易事。

三、对“损害”的界定应与风险规制理论相契合

从以上个人信息侵权案例反映的情况来看，审判实务中的问题主要围绕损害类型展开。按照损害赔偿的基本原理，受害人主张损害赔偿责任时需要证明自身遭受了法律上可补救的损害，〔16〕而信息风险性损害能否被纳入法律上的损害范畴，已成为信息主体寻求私法救济的阻碍。《民法典》第1165条第1款作为侵权责任的一般条款，仅提及“损害”一词而未否定风险成立损害的可能性，因此，本部分将从风险规制视角出发，探讨信息风险构成损害的正当性。

（一）风险规制路径：风险控制和风险分配

自20世纪伊始，伴随科技的多次革命性飞跃，愈益频繁爆发的风险致害造成的大规模损害引发人们对工业社会法律思维模式的批判，在此背景下，德国思想家乌尔里希·贝克首倡“风险社会”理论。风险社会中的“风险”是与自然风险（如各种自然灾害）相对应的风险，其内在于科学技术，“可被定义为以系统的方式应对由现代化自身引发的危险和不安”〔17〕。随着科学技术的广泛应用，人类面对和遭受的风险数量和级别大大提高。就风险分布而言，尽管有权势和财富的社会阶级也不能逃脱风险的危害，但若不通过法律、政策对风险进行控制或分配，那么将形成风险与财富呈反比分配的不公状态。〔18〕基于此，国家的任务转向“以未来为目标的对科技发展

〔13〕 参见北京市顺义区人民法院（2020）京0113民初字第16062号民事判决书。

〔14〕 参见湖南省益阳市赫山区人民法院（2021）湘0903民初字第1506号民事判决书。

〔15〕 参见北京市第三中级人民法院（2020）京03民终字第2049号民事判决书；北京互联网法院（2018）京0491民初字第1905号民事判决书。

〔16〕 参见王叶刚：《论侵害人格权益财产损失赔偿中的法院酌定》，载《法学家》2021年第3期。

〔17〕〔德〕乌尔里希·贝克：《风险社会：新的现代化之路》，张文杰、何博闻译，译林出版社2018年版，第7页。

〔18〕 参见何国强：《风险社会、风险分配与侵权责任法的变革》，载《广东社会科学》2018年第3期。

可能给社会造成的危险进行预防”〔19〕，即如何规制风险成为现代国家的一项重要任务。根据公共性程度可将风险分为公共风险和个体风险两类，〔20〕两类风险的特点决定了规制方式的差异。个体风险是指“那些分散制造的，地方化的，可受个人控制或者是来自本体的风险”〔21〕，由于该风险的主体关系单一且损失相对固定，法律能够做到通过个案判断对个体风险进行分配与化解。因此，规制个体风险的路径是风险分配，重心在于对被害人的风险损害予以赔偿。而公共风险其实是个体风险扩散的结果，具有广泛的扩散性、蔓延性，显然难以简单依靠传统的私人自治或市场机制来防控。相较于个体风险而言，在公共风险的规制上，应注重从整体上控制风险的蔓延和扩张，即通常采取以追求秩序为价值取向的风险控制路径。风险控制路径和风险分配路径之间存在互补性的特点，前者是一种事前的规制思维，后者是一种事后的规制思维。鉴于此，在将风险作为规制目标时，常规的风险规制做法是并行适用上述两种路径，进而发挥出两种路径融合规制风险的优势。

（二）引入风险分配路径的方式：认可信息风险性损害

在大数据背景下，人们对数据、信息的依赖导致风险不可避免地裹挟而至，信息流转共享本身即是一种典型的社会风险活动，这可从《个人信息保护法》多次使用“风险”概念中得到证实。因此，法律对个人信息的规范面临着如何有效平衡信息安全保障与信息流转共享之间的关系，即在最大程度地满足信息处理者对信息需求的情况下，通过设置合理的风险控制或者风险分配路径，避免信息主体在信息处理活动中承受不合理的风险。

个人信息具有典型的复合法益性质，信息之上不仅汇集了各方主体不同类型和性质的利益诉求，各类风险也相应伴生于各方主体的活动之中。就公共风险而言，我国现行规范规定的风险控制路径较为多元，不仅通过《刑法》《治安管理处罚法》等公法来达到风险控制的效果，更是在《个人信息保护法》中明确规定了国家网信部门承担的监督管理义务，个人信息处理者承担的风险评估、告知同意等义务，来应对个人信息领域的公共风险。但受社会认知的限制，在采取风险控制措施的情况下仍存在剩余风险的可能，这就涉及风险分配的问题。

鉴于“从危险中获取经济利益者也经常被视为具有制止危险义务的人”〔22〕，剩余风险理应由作为信息风险之源与主要获益者的信息处理者承担。按照法经济学理论，“纯粹的风险分配与损害分配是重合的”〔23〕，亦即在剩余风险转化为现实的诈骗、身份窃取等损害之前，信息处理者所承担的风险在资本逻辑中可通过赔偿的方式进行转移。然而，信息风险性损害与传统侵权损害概念的抵牾阻断了风险性损害的转移，这使得信息主体以私法手段特别是侵权责任手段寻求损害赔偿的整体效果不尽人意。归结而言，信息风险分配路径的缺位导致司法实务中频现信息损害认定难的问题，因此，在风险控制的基础上引入风险分配路径成为必要，而将满足特定条件的信息风

〔19〕〔德〕乌尔里希·巴斯特：《德国行政法读本》，于安等译，高等教育出版社 2006 年版，第 53 页。

〔20〕参见侯东德、周莉欣：《风险理论视角下智能投顾投资者的保护路径》，载《华东政法大学学报》2021 年第 4 期。

〔21〕Peter Huber, Safety and The Second Best: The Hazards of Risk Management in the Courts, 85 *Columbia Law Review* 277, 278 (1985).

〔22〕〔德〕克雷斯蒂安·冯·巴尔：《欧洲比较侵权行为法》（下册），张新宝译，法律出版社 2001 年版，第 271 页。

〔23〕前引〔18〕，何国强文，第 233 页。

险性损害视为法律上承认的损害，无疑是一种高效的风险分配路径。

（三）认可信息风险性损害的正当性：符合风险分配正义

风险分配实质上是“风险成本、风险责任、风险损失在主体间的承担”〔24〕，由于风险具有不利益，为确保数字经济的健康发展，风险分配必须把实现正义作为最重要的目标追求。在个人信息保护的问题上，认可信息风险性损害不仅阻断了不公平分配风险现象的扩展，又能包容性地促进新兴信息产业的发展。具体而言：其一，认可信息风险性损害意味着让真正制造风险且获取收益的主体承担风险。个人信息侵权损害极少伴随着信息主体财产、人身受损等直接物质性损害，通常带来的是外部风险或焦虑不安等非物质性损害，该类损害具有不确定性、无限性和难以计量等特点。由于风险性损害与侵权法框架下的多数损害特征以及人们对损害的一般认识存在差异，法院常以损害不存在为由驳回受害人的损害赔偿请求，这等于纵容了信息处理者肆无忌惮地使用信息，并将风险转嫁给无辜且缺乏预防能力的信息主体。认可信息风险成立损害，并将损害分配给风险预防能力较高的信息处理者，客观上遏制了风险分配的不公现象，有助于保障处于弱势地位的信息主体的权益。其二，认可信息风险性损害具有预防风险的功能，有利于保障社会整体利益。风险分配正义以实现多数人的合法利益为目的，即通过合理的制度安排使风险对公众的总体损害降至最低。〔25〕相较于个人信息主体，信息处理者掌握更多资源和技术，在风险预防方面处于能力更强的位置，可以通过采取提高产品质量或采购风险防控设备等方式分散风险。而认可信息风险性损害相当于一种事后的惩戒机制，能够倒逼个人信息处理者积极采取上述措施，从而达到预防信息风险的目的。

事实上，司法实践中，风险性损害在环境污染、医疗损害赔偿、毒物侵害等领域已经得到认可与适用。在比较法上，欧盟立法也采用了抽象的损害概念，信息主体因数据泄露而导致身份盗窃或欺诈、声誉受损等非物质性损害，都有权要求信息处理者承担损害赔偿责任，〔26〕《德国联邦数据保护法》第 83 条第 2 款与《印度个人数据保护法案》第 3 条第 20 项同样也认可了个人信息风险性损害。

四、以信息损害为中心续造损害赔偿规则

损害与赔偿如影随形，是开启损害赔偿的“钥匙”。鉴于个人信息风险性损害的特点及既有损害赔偿规范的不足，为使事实上的信息损害真正转变为可获合理赔偿的法律上的损害，仍需回应信息风险性损害的具体样态、精神损害赔偿的条件以及损害赔偿数额的计算规则等问题。

（一）明确信息风险性损害的样态和识别因素

1. 风险性损害的具体样态

损害是权利或利益被侵害的后果，我国现有法律规范并未就损害这一概念进行正面界定。在

〔24〕 徐钝：《社会风险分配失衡的社会资本矫正——以法理型社会资本培育为中心》，载《学术论坛》2013 年第 7 期，第 70 页。

〔25〕 参见张晒：《风险分配何以公正？——基于新冠肺炎疫情的哲学审思》，载《北京理工大学学报（社会科学版）》2020 年第 3 期。

〔26〕 参见解正山：《数据泄露损害问题研究》，载《清华法学》2020 年第 4 期。

损害赔偿法的历史上，“差额说”一直占据着重要地位，〔27〕认为对损害的界定起决定性作用的并非具体法益遭受的侵害，而是受害人在侵权行为发生后实际享有的利益状态（减数）与若侵权行为未发生时的假设利益状态（被减数）之差额。因此，在判断信息风险性损害的样态时，可凭借“差额说”将信息风险性损害具体化为信息主体遭受的各种损害。

（1）外部风险性损害：附带财产损失

个人信息具有“可识别性”，且基因信息、生物识别信息等敏感信息又是不可更改和删除的，一旦暴露，将给信息主体带来身份被窃取或欺诈的风险。而个人信息在网络空间中又具有传播的即时性和复刻的便利性等特征，这使得信息主体面临未来遭受损害的风险升高。为避免未来损害的发生，信息主体通常会采取预防措施来应对风险，如购买风险监控服务、更换手机号等，以及因个人信息侵权行为而增加诉讼费、误工费等合理诉讼支出，这些实质上可被视为信息风险性损害。预防费用、诉讼成本支出等附带财产损失在性质上虽为“自愿的支出”，但这些费用在个人信息被侵权之前是无需支出的，在侵权行为发生之后则成为必要，且其中有些诉讼成本支出具有风险预防性质，实质上可被扩大解释为《网络侵权司法解释》第 12 条第 1 款规定中所称的“被侵权人为制止侵权行为所支付的合理开支”。〔28〕事实上，依《民法典》第 995 条规定的消除危险等人格权请求权，信息主体本就可向信息处理者主张消除危险等责任，若受害人已经采取相应措施，支出的合理预防费用和具有风险预防性质的诉讼成本支出当然构成事实上的损害。外部风险性损害直观传达的是一种面向未来的可能性，而将上述附带财产损失视为外部风险性损害，除了能够按照合理财产损失的标准对外部风险进行量化外，亦能增强信息主体界定信息损害赔偿范围的可预期性，从而调动个人采取预防措施的积极性，有助于避免更大损害的发生。

（2）风险引发的内心焦虑：精神损害

“精神损害是指受害人在人格权或其他权利受到侵害后，而遭受的生理痛苦、精神痛苦以及其他不良情绪。”〔29〕循此定义及《民法典》第 1183 条的规定可知，精神损害赔偿救济的对象是人格权、身份权和人格利益、身份利益等人身权，基本形态包括身体疼痛和精神痛苦。尽管《民法典》《个人信息保护法》等规范将个人信息的保护层级界定为法益而非权利，但因个人信息权益属于人格利益而可通过精神损害赔偿获得救济，且其损害形态往往归于精神痛苦。实务中，通过隐私权保护逻辑获得精神损害赔偿自无争议，法律适用的最大瓶颈在于焦虑不安等精神状态能否构成精神损害。信息主体因信息泄露而使身份或财产处于风险之中的常态反应，通常是无法言明的担忧或焦虑等消极精神状态，与确定的身体疼痛和因侵犯隐私权或名誉权引起的精神痛苦相比，并不那么直观而不易被认可。其实，在个人信息特别是生物识别信息、行踪信息等敏感信息因泄露而发生现实损害之前实为一颗“不定时炸弹”，涉及此类信息的侵权行为无疑破坏了个人

〔27〕 参见徐建刚：《〈民法典〉背景下损害概念渊流论》，载《财经法学》2021 年第 2 期。

〔28〕 参见杨立新：《侵害个人信息权益损害赔偿的规则与适用——〈个人信息保护法〉第 69 条的关键词释评》，载《上海政法学院学报》2022 年第 1 期；田野：《风险作为损害：大数据时代侵权“损害”概念的革新》，载《政治与法律》2021 年第 10 期。

〔29〕 张新宝：《精神损害赔偿制度研究》，法律出版社 2012 年版，第 17 页。

生活安宁和安全稳定预期。由此产生的焦虑随着时间的流逝，足以造成精神损害。〔30〕此外，在信息侵权领域，因大规模数据泄露而频繁发生的受害者遭受财物或其他严重财产损失的事件表明，〔31〕还未遭受现实损害的信息主体对风险的担忧并非凭空产生的心理压力，损害后果不言而喻，因此，认可内心焦虑属于精神损害并具有可赔偿性无疑是大数据时代的大势所趋。

2. 确定风险性损害的参考因素

承认信息风险性损害具有正当性，但风险性损害是否确定发生应建立在合理可靠的未来风险预测基础之上。法官对个案中风险性损害的预判取决于未来的信息流通过程，应由法官参考相关因素裁量确定。具体而言，对风险性损害的认定有影响的因素主要包括如下几项：（1）个人信息的种类。个人信息被侵害后成立风险损害的可能性与信息的性质相关，一般而言，私密或敏感信息相较于一般信息更具重要性，故其被侵权后造成的风险更容易成立损害。因此，在我国信息风险性损害的认定普遍艰难的现状下，基于现行立法在私密或敏感信息的处理上以禁止为原则，以有条件允许为例外的立场之考量，〔32〕对个人信息保护采取分而治之的策略极有必要，即私密或敏感信息的暴露本身即视为“现实损害”，对一般个人信息风险需满足特定条件才予以认可成立损害。（2）信息处理者的主观目的。在无形的网络空间中，信息处理者实施侵害行为时的主观状态对损害的判断至关重要，该主观状态一般可通过间接的方式推知。例如，在黑客攻击导致的数据泄露事件以及因平台收集数据产生的消费操控或歧视等侵权案件中，侵权人恶意获取或违法使用个人数据的主观故意是非常明显的，即使未立即利用获取的信息开展欺诈或歧视等下游侵权行为，违法使用信息是迟早的事，认可该种情形下的风险成立损害具有合理性。（3）信息侵权损害的迹象。风险性损害具有伴随时间的推移逐渐显现的特点，若在同一信息泄露活动中已有部分信息主体遭受身份窃取或欺诈，这表明尚未遭受现实侵害的信息主体在未来也有受到类似损害的风险，这可成为法官裁量的重要参考因素。当然，现实中个人信息风险的情形千差万别，法院裁定参考因素的类型无法一一列举，司法实践中还需由法官根据个案的具体场景综合判断。

（二）适当缓和可获赔偿的精神损害程度要求

精神损害赔偿意味着受害人能够通过金钱来缓解精神痛苦，更为关键的是实现了身体与灵魂在法律上的平等对待。〔33〕认可信息风险引发的内心焦虑成立精神损害，意味着信息主体可通过内心焦虑损害及隐私权损害两种途径主张精神损害赔偿，而以“严重”作为获取精神损害赔偿的条件，无疑将造成损害赔偿与精神损害之间的逻辑断裂。从理论视角观之，“严重”要件的基础主要是侵权法上的“忽略轻微损害”规则和现代侵权法中的“水闸理论”，两者都以协调权利保护与行动自由为目的。〔34〕然而，随着人们对人格尊严的逐渐重视，该限制条件的正当性正在受到挑战。其一，有违精神性人格权高于财产权利的民事权益位阶理论。精神层面的权益保护映射

〔30〕 See DJ. Solove，DK Citron，Risk and Anxiety：A Theory of Data Breach Harms，96 *Texas Law Review* 737，765 (2018).

〔31〕 参见湖南省张家界市中级人民法院（2021）湘08刑终字第112号刑事裁定书；云南省楚雄彝族自治州中级人民法院（2021）云23刑终字第229号刑事裁定书。

〔32〕 参见《民法典》第1033条，《个人信息保护法》第28条。

〔33〕 参见谢鸿飞：《精神损害赔偿的三个关键词》，载《法商研究》2010年第6期。

〔34〕 参见李昊：《纯经济上损失赔偿制度研究》，北京大学出版社2004年版，第53页。

出人类文明的发展程度，从《民法典》人格权编的规定可推知，“与其他法益，尤其是物质性的利益相比，人的生命和人格尊严处于更高的位阶”〔35〕，亦即精神性人格权因属高于财产权利的民事权益理应获得优先保护。〔36〕但现实是被侵权人主张财产损失赔偿并不以“严重”为限制条件，而是奉行全部赔偿原则（包括轻微损害），且在人身伤害案件中的精神损害赔偿请求通常都会被支持。与之相反，尽管当事人所受的精神痛苦在非物质性人身权益的损害中有可能处于唯一地位，立法仍以“严重”这一高门槛作为获得精神损害赔偿的前提条件，这不仅使得介于微小与严重之间的精神损害无法获得赔偿，更会变相助长侵权人侵权的动力。其二，非以“严重”作为限制条件并不会引发大量精神损害赔偿请求如洪水般涌向法院。从实证层面考察，对于真正受到精神痛苦的受害人而言，其坚持诉讼并不以赔偿金的数额为主要目的，而是“有”或者“没有”获得赔偿金。恶意诉讼主体虽以追求高额损害赔偿为目的，但赔偿金数额普遍并不高的现实会使其丧失诉讼的动力，所以无需过度担忧诉权被滥用。

此外，从比较法视角观之，《德国民法典》第 253 条未将“严重”作为适用精神损害赔偿的法定条件，欧盟《一般数据保护条例》第 82 条第 1 款与德国《联邦数据保护法》第 83 条第 2 款，也体现了取消精神损害严重性要求、降低精神损害赔偿门槛的趋势。〔37〕就我国而言，可获赔偿的精神损害的适用范围呈逐步扩大的趋势，如《民法典》肯定了违约精神损害赔偿、侵害“具有人身意义的特定物”的精神损害赔偿等，凸显了立法对人格尊严的重视。因此，为确保个人信息处理不逾越人格尊严底线，降低精神损害赔偿的条件实属必要。当然，适当降低精神损害严重性的条件并不意味着对精神损害的一概承认，而使信息处理者动辄因显著轻微的权益损害行为对信息主体赔偿精神损害，被侵权人因个人信息侵权而主张精神损害赔偿请求时，仍应向法院提供其遭受精神压力或痛苦的初步证据。

（三）厘清信息损害赔偿数额的计算规则

1. 损害赔偿数额的计算依据

损害赔偿责任的落实依赖于损害赔偿数额的计算依据。《个人信息保护法》第 69 条第 2 款借鉴了《民法典》第 1182 条规定的计算方法，将信息主体“受到的损失”和信息处理者“获得的利益”在适用顺位上合并为同一层次，赋予受害人在损害赔偿与返还获利之间进行选择的权利以实现保护的最大化，当根据以上两种计算方法难以确定赔偿数额时，则由法院“根据实际情况确定”。当个人信息因权益被侵害而遭受财产损失时，依据该计算规则主张损害赔偿数额自不待言，问题在于，《民法典》第 1182 条规定的损害赔偿性质是侵害他人人身权益造成的财产损失而非精神损害，那么，《个人信息保护法》第 69 条规定的损害赔偿性质如何呢？这涉及精神损害赔偿数额的计算依据。

上已述及，在个人信息侵权领域，风险引发的内心焦虑能够成立精神损害，这表明《个人信息保护法》第 69 条第 1 款中的“损害赔偿”应当包括精神损害，而第 2 款规定的计算方法又是针对第 1 款中的损害赔偿责任设计的，因此，无论是财产损失还是精神损害，都可以按照第 2 款的规定确定赔偿数额。但由于“受到的损失”和“获得的利益”这两种计算方法的侧重点不同，

〔35〕〔德〕卡尔·拉伦茨：《法学方法论》（第六版），黄家镇译，商务印书馆 2020 年版，第 421 页。

〔36〕参见王利明：《论民事权益位阶：以〈民法典〉为中心》，载《中国法学》2022 年第 1 期。

〔37〕参见张建文、时诚：《个人信息的新型侵权形态及其救济》，载《法学杂志》2021 年第 4 期。

财产损失和精神损害在具体计算规则的适用上存在差异。通说认为，“受到的损失”应被解释为财产损失，不宜扩张至精神损害，〔38〕这意味着“受到的损失”这一计算方法侧重救济的是个人信息权益人受到的财产损失，排除了精神损害赔偿责任通过该计算方法得以落实的可能。就“获得的利益”而言，利益是指个人信息处理者侵害个人信息权益获得的财产利益，而精神损害赔偿责任的最终体现方式是支付精神损害抚慰金，因此，将“获得的利益”作为落实精神损害赔偿责任的计算方法更为妥当，有助于解决精神损害难以量化之难题。所谓“根据实际情况确定赔偿数额”，其实是指由法院依职权酌定赔偿数额，财产损失和精神损害均是法官酌定的对象。需要注意的是，法官在酌定时的考量基础除了信息主体“受到的损失”和信息处理者“获得的利益”外，还需要“根据侵权人的过错程度、具体侵权行为和方式、造成的后果和影响等确定”〔39〕。

2. 惩罚性赔偿数额的确定

就个人信息侵权损害赔偿责任而言，除部分案件中存在能够按照合理财产损失的标准进行量化的预防风险支出和维权成本等实际损害外，多数案件中的信息损害具有个体损失数额较小的特点。在个人信息侵权行为发生后，若仅以单个个人信息的实际价值来计算赔偿数额，每笔赔偿 1 元或 2 元，这样的结果不仅不能惩治信息处理者利用个人信息非法获利的行为，也难以调动权利人维权的积极性，因此，有必要在个人信息侵权损害赔偿责任中规定惩罚性赔偿责任。“惩罚性赔偿又称报复性赔偿，是指由法院判决作出的赔偿数额超出实际损害数额，对侵权人具有惩罚功能的损害赔偿责任。”〔40〕相较于《侵权责任法》，《民法典》将惩罚性赔偿的适用范围扩展至知识产权和破坏生态领域，表明《民法典》注重对恶意侵权行为进行惩罚的态度。事实上，欧盟《一般数据保护条例》第 83 条已就高额罚款作出了规定，在英国的司法实践中，也存在因航空公司泄露乘客信息而被开出 1.839 亿英镑罚款的案例。〔41〕一旦明确应当在个人信息侵权领域设置惩罚性赔偿责任，就涉及惩罚性赔偿数额的确定问题。对此，应当从计算基数和倍数两方面着手。计算基数的一般规则应当是依照侵权行为造成的实际损失计算，〔42〕根据《个人信息保护法》第 69 条第 2 款的规定，在个人信息侵权领域，惩罚性赔偿的计算基数应当是信息主体“受到的损失”和信息处理者“获得的利益”。关于计算倍数，在已成熟适用惩罚性赔偿的知识产权、消费者权益保护等领域，并未形成统一的标准，但基本处于 1～5 倍之间，因此，信息侵权惩罚性赔偿中的计算倍数可由法官在 1～5 倍的范围内自由裁量。

综上可知，在个人信息侵权行为发生后，个人信息处理者需要对财产损失、精神损害、惩罚性赔偿承担责任。但由于多数信息侵权案件中被侵权人受到的损失较微小，按照计算依据得出的上述三种赔偿数额的总和通常也不能达到惩罚恶意侵权人的目的，因此，实行损害赔偿最低赔偿标准就十分必要。我国台湾地区“个人资料保护法”规定，每人每事件新台币 500 元以上 2 万元以下计算，美国《加州消费者隐私法案》所认定的赔偿范围是 100 美元至 750 美元之间。〔43〕其实，我国《消

〔38〕 参见王利明：《民法》（下册），中国人民大学出版社 2020 年版，第 532 页。

〔39〕 黄薇：《中华人民共和国民法典侵权责任编释义》，法律出版社 2020 年版，第 57 页。

〔40〕 杨立新：《〈民法典〉惩罚性赔偿规则的具体适用》，载《荆楚法学》2022 年第 1 期，第 65 页。

〔41〕 参见孙莹：《大规模侵害个人信息高额罚款研究》，载《中国法学》2020 年第 5 期。

〔42〕 参见前引〔40〕，杨立新文。

〔43〕 参见刘云：《论个人信息非物质性损害的认定规则》，载《经贸法律评论》2021 年第 1 期。

费者权益保护法》《食品安全法》也早已规定了损害最低赔偿标准，分别是 500 元和 1000 元。就侵害个人信息的微额损害而言，因个人信息可被进一步分为普通和敏感两类，结合现行法在产品、食品领域的微额损害赔偿标准的规定，侵害普通信息时可以按照每人每事件 500 元，侵害敏感信息时可以按照每人每事件 1000 元，如此方能确保被侵权人的维权成本和胜诉利益之间的平衡。

五、结　语

在大数据时代，被转化为数据的海量个人信息是云计算、区块链等尖端科技的“燃料”，如何实现个人对自身信息的“脱控”而不“失控”，所受损害得到充分救济是法律适用最为关注之点。对此，《个人信息保护法》在以往信息保护规范的基础上全面规定了个人信息保护规则，但因个人信息侵权损害与传统侵权法上的损害认定标准间的不匹配性，通过私法保护个人信息的司法实践力有不逮。在风险社会背景下，立法者不应仅将着眼点置于非赔偿性民事责任，还应当在潜在损害风险转化为诈骗等现实损害之前对风险进行分配，即通过损害赔偿责任对信息主体承担的风险损害进行补偿。诚然，对风险性损害的认可无疑将对法律适用的稳定性造成一定程度的冲击，因此，笔者又从信息风险性损害的具体样态、精神损害赔偿的条件以及损害赔偿数额的计算依据等方面进一步完善了信息损害赔偿规则，以期能够破解个人信息权益保护之司法难题。

Abstract: As one of the civil liabilities for the relief of personal information rights and interests damage, the liability for damages has a core position in the system of tort liability. However, empirical data and case analysis show that the judicial practice of information protection takes a strict attitude towards the application of liability for damages, and the differences and difficulties in the identification of damages have become the primary obstacles for information subjects to seek relief of private law. From the perspective of risk regulation theory, it is an efficient way of risk distribution to bring information risk damage into the category of legal damage, and it is also an effective way to solve the dilemma of private law protection. In addition, in order to ensure the implementation of the liability of information tort damages, we should rely on the “difference theory” to concretize the information risk damage into collateral property loss and mental damage caused by anxiety. We need to take appropriate mitigation of the severity of mental injury requirements, and clarify the calculation rules of the amount of compensation for property loss, spiritual damage and punitive damages, so as to make compensation for damages play a better function of filling the loss.

Key Words: personal information rights, risk damage, rules for damages, punitive damages

（责任编辑：徐建刚　赵建蕊）

财经法学 No. 5，2022
pp. 81 - 94

论超大型平台独立机构的功能构造
——以《个人信息保护法》第58条为中心

韩　阳*

内容提要：《个人信息保护法》第58条第1项规定超大型平台企业应成立主要由外部成员组成的独立机构对个人信息保护情况进行监督，目前存在三种制度设计方案。第三方独立机构方案比较优势不明显，不符合风险预防理念，难以承载监督功能期待，因此应当被舍弃。管理监督型独立机构方案属于日常性合规管理模式，是董事会对经理层的管理监督，独立机构在董事会领导下开展活动，无法解决合规动力问题，难以厘清董事会与执法机构之间的紧张关系。决策监督型独立机构方案属于危机性合规整改模式，是执法机构对董事会的整改督导，组建董事会专门委员会，依托独立董事进行内部控制，但独立董事法律责任模糊，容易造成董事会负担过重。两种方案各有优劣侧重，应当区分问题场景分别应用，实现对公民个人信息的系统性和持续性保护。

关键词：超大型平台　独立机构　管理监督　决策监督

一、问题的提出

为加强超大型平台监管，我国《个人信息保护法》新增了独立机构这一制度要求。《个人信息保护法》第58条第1项规定，提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督。问题随之而来：独立机构的功能定位、人员构成、权利义务和法律责任应如何设计？怎样保持该机构的独立性？如何实现有效监督？本文尝试对此进行探索。

为什么要求超大型平台成立独立的监督机构？与个人信息保护负责人是什么关系？缘何独立

* 韩阳，北京大学法学院博士研究生。

机构主要由外部成员组成呢？对于这些问题，立法资料显示“有的部门、专家建议，强化超大型互联网平台的个人信息保护义务，并加强监督”，全国人大宪法和法律委员会经研究建议增加这一款。〔1〕2021 年 8 月 20 日，经过三次审议，十三届全国人大常委会第三十次会议表决通过了《个人信息保护法》，全国人大常委会法工委经济法室副主任杨合庆对《个人信息保护法》进行了解读。他表示：“为了提高大型互联网平台经营业务的透明度，完善平台治理，强化外部监督，形成全社会共同参与的个人信息保护机制……个人信息保护法对这些大型互联网平台设定了特别的个人信息保护义务。”〔2〕由此可见，我国立法机关将独立机构的功能定位为外部监督，通过多元主体参与构建平台治理的开放式关系结构。

从法律条文看，独立和监督是该机构的两个显著特征，外部是对组成人员的要求。监督是该机构的功能定性，是设计这一机构的出发点和落脚点。独立性包含组织独立、职权独立和人员独立三个方面。只有在监督者和监督对象都明确的前提下，是否独立才能够最终研判。如何实现独立监督呢？学界和实践中存在三种方案，分别是第三方独立机构方案、管理监督型独立机构方案和决策监督型独立机构方案，以下分别进行讨论。部分方案内容较少，本文尝试进行拓展并做利弊分析。

二、第三方独立机构方案

在《个人信息保护法》生效前，部分超大型平台企业已经进行了初步尝试。腾讯在 2021 年 10 月 15 日公开招募外部成员，组建个人信息保护外部监督委员会，文字表述为“第三方独立监督机构”，职责包括独立评议腾讯公司及各产品隐私保护相关工作、提出指导和修改建议等。“委员会首批成员为 15 个人左右，计划包括法学专家、技术专家与行业协会等个人信息保护领域的专业人士，也将涵盖律师、媒体等其他公众。首批成员将通过公开招募和定向邀请等方式产生。”〔3〕携程在 2021 年 10 月 25 日发布公告，决定近期成立“个人信息保护外部监督专家团”，同样表述为“第三方独立机构”。〔4〕在外部监督的功能定位下，超大型平台希望通过第三方独立机构的形式实现外部监督效果，将独立性理解为“外部独立”，监督机构独立于本平台企业。但这种做法比较优势并不明显，不符合风险预防的治理理念。

第一，《个人信息保护法》第六章专门规定了履行个人信息保护职责的部门，这些职能部门完全独立于企业，属于纯粹外部监督的国家机构。无论立法目的追求的是“独立性”或是“监督性”，负有监管职责的国家机关都是最佳主体，而不是所谓的第三方独立机构。近年来行政执法强调柔性执法和治理导向，存在许多企业发声和公众参与的合法渠道。反观这些所谓的独立机

〔1〕 参见《全国人民代表大会宪法和法律委员会关于〈中华人民共和国个人信息保护法（草案）〉修改情况的汇报》。

〔2〕 朱宁宁：《8 章 74 条，个人信息保护法来了！权威解读十大亮点》，载 https://mp.weixin.qq.com/s/Y-031EBzOsbbN2JAEcOGBQ，最后访问时间：2022 年 7 月 23 日。

〔3〕《这是一封来自鹅厂隐私官的邀请函，请查收！》，载 https://mp.weixin.qq.com/s/2ZvcExeY_l-J3dfw02zTFg，最后访问时间：2022 年 7 月 23 日。

〔4〕 参见《携程“个人信息保护外部监督专家团”招募公告》，载 https://view.inews.qq.com/a/20211025A093AW00，最后访问时间：2022 年 7 月 23 日。

构，实际上难以摆脱超大型平台的干扰，平台企业主导之下的民主参与和监督强度都存在问题。用户代表或公众代表的产生，专家学者的挑选，都有可能被超大型平台把持，使所谓的独立监督机构沦为平台权力的装饰。

第二，即便追求平台治理的多元参与，实际上也并无必要。现实中已经广泛存在着第三方独立机构，各类行业协会、学会智库和科研高校等等，如在 APP 专项整治活动中发挥作用的中国网络空间安全协会，每年发布个人信息保护测评报告的北京大学互联网法律中心。这些机构或独立存在，或由政产学研媒一同发起成立，各大头部平台企业也参与其中。它们定期发布研究报告，组织企业调研、立法研讨和独立监督，实际上已经发挥了社会监督的客观作用。这些社会组织通过内部章程对成员形成约束力，通过法律程序获得登记备案，不需要专门立法予以合法性确认。这些社会组织的经费人员更具有独立性，它们通过声誉机制和竞争机制进行自我监督，相较企业自设机构具有一定的制度优势。

第三，外部监督无法实现事前事中监管，难以有效影响超大型平台企业决策。如果按照两家企业的制度设想展开，独立机构对超大型平台进行形式监督，仅仅作出指导、提出建议和咨询培训，那么独立机构极容易沦为装饰企业形象的花瓶，监督功能将被完全掏空。独立机构无法深入平台企业内部决策，否则就将与外部监督的职能定位相冲突。超大型平台企业的各种业务和不同流程都与个人信息有关，个人信息被滥用有时候只是一个最终结果，更多问题可能出在事前决策和事中执行。尤其是很多敏感个人信息，如生物识别信息，一旦被泄露滥用将会给自然人带来不确定风险。有学者提出：“区别于传统的‘危险’，个人生物识别信息应用风险具有不确定性与复杂性，因果关系具有模糊性与非线性，损害具有严重性与不可逆性，因此政府监管理念应当从消极的‘危险消除’向积极的‘风险预防’转变。”〔5〕

三、管理监督型独立机构方案

该方案由张新宝教授提出，主张“作为企业内部的‘独立监督机构’，主要是指独立于企业的日常经营管理机构（如总经理）、产品或者服务研发推广机构等业务部门，因为这些机构和部门往往会以利润导向进行管理和经营而忽视个人信息保护”〔6〕。该方案下独立机构包含两项具体职责：其一，监督大型互联网平台企业自身的个人信息保护合规情况；其二，监督大型互联网企业对商业用户的个人信息处理活动予以规范的合规情况。〔7〕除此之外，独立机构在董事会的领导下，还有提出建议和合规指导的功能。超大型平台的业务部门是该方案的预设监督对象，本质是董事会对经理层的管理监督。数据合规在我国仍处于发展初期，该方案有助于专家参与企业合规制度建立，同时制度上防范经理层和业务部门的数据滥用行为，方案内容丰富具有很强的操作性和执行性。在讨论独立机构与国家个人信息保护部门的关系时，张新宝教授主张：“独立监督机构对企业个人信息保护事项作出的决定或者提出的鉴定意见，原则上将得到国家个人信息保护

〔5〕 于洋：《论个人生物识别信息应用风险的监管构造》，载《行政法学研究》2021 年第 6 期，第 111 页。

〔6〕 张新宝：《大型互联网平台企业个人信息保护独立监督机构研究》，载《东方法学》2022 年第 4 期，第 44 页。

〔7〕 参见前引〔6〕，张新宝文。

部门的认可。在发现企业在个人信息保护方面存在重大隐患或者严重违法情形时，独立监督机构应当及时向企业的权力机构提出意见和建议。企业权力机构拒绝接受的，经独立监督机构多数成员表决同意，应将相关情况报告国家个人信息保护部门。”〔8〕这一制度设计极大增强了独立机构的实际权力，仿佛达摩克利斯之剑一样悬在超大型平台企业头顶。但是产生两个问题需要解释：第一，如果独立机构受董事会领导，为什么决定和鉴定意见要征得监管部门认可，为什么可以越过董事会，直接向监管部门报告；第二，如果独立机构照此运行，会不会干扰企业的自主经营活动。

在规制理论中，该方案属于内部管理型规制理论（management-based regulation）〔9〕的实际运用，“实际上是行政权对企业内部治理的介入，在实质上构成对企业经营自主权的限制”〔10〕。对于内部管理型规制，国外学者将生产流程划分为规划、执行和产出三个部分，在不同阶段采取的规制策略，被称作内部管理型规制、技术标准规制（technology-based regulation）和绩效标准规制（outcome-based regulation）。根据内部管理型规制，公司应制定符合一般标准的计划，以促进有针对性的社会目标。监管标准规定了每个计划应该具备的要素，如危险识别、风险防范措施、监测纠正程序、员工培训政策，以及其他社会目标评估和完善公司管理的具体措施。〔11〕“内部管理型规制不规定特定的技术要求或绩效结果，而是要求企业针对行政目标，制定适合自身的内部经营计划、管理流程及决策规则，从而将社会价值内部化。”〔12〕这一规制类型属于元规制（meta regulation）的典型类型，与自我规制具有高度关联性。“元规制是指外部规制者有意促使规制对象本身针对公共问题，作出内部式的、自我规制性质的回应，来要求或塑造规制对象的自我规制。”〔13〕

结合内部规制理论，该方案具有三点积极意义：第一，针对个人信息风险，应该采用风险预防的规制策略。“互联网的复杂结构以及大数据处理过程随机性、相对性和模糊性特征，表明数据主体基于个人信息与数据控制者建立的信息关系影响因素存在高度的不确定性。传统规制模式以规则为规制工具，通过行为和结果的确定性联系进行危险排除，并不符合数字时代信息分享的风险特征。”〔14〕第二，当风险不明、标准不清时，实际上难以判断个人信息是否被滥用泄露，事后监督难以挽回实际损失。需要深入平台企业内部，对个人信息管理体系进行优化改造，政府规制视角应该由外入内。第三，个人信息保护问题异质性强，平台、部门和流程之间都不一样，需要编制细密的行动规范。但是，个人信息保护法律制度建立初期，诸多制度细节、技术标准和行

〔8〕 前引〔6〕，张新宝文，第 48 页。

〔9〕 也有学者将其翻译为“以管理为基础的规制”或“基于管理的规制”。参见洪延青：《“以管理为基础的规制”——对网络运营者安全保护义务的重构》，载《环球法律评论》2016 年第 4 期；高秦伟：《社会自我规制与行政法的任务》，载《中国法学》2015 年第 5 期。

〔10〕 孔祥稳：《论个人信息保护的行政规制路径》，载《行政法学研究》2022 年第 1 期，第 144 页。

〔11〕 See Cary Coglianese & David Lazer, Management-Based Regulation: Prescribing Private Management to Achieve Public Goals, 37 *Law & Society Review* 694 (2003).

〔12〕 谭冰霖：《论政府对企业的内部管理型规制》，载《法学家》2019 年第 6 期，第 75 页。

〔13〕〔英〕罗伯特·鲍德温、马丁·凯夫、马丁·洛奇：《牛津规制手册》，宋华琳等译，上海三联书店 2017 年版，第 167 页。

〔14〕 谢尧雯：《基于数字信任维系的个人信息保护路径》，载《浙江学刊》2021 年第 4 期，第 82 页。

业要求都需要进一步明确。因此，应将规则自由裁量权下放给企业，监管机构不宜采取硬标准强要求。

但是，运用内部规制理论分析建构超大型平台独立机构，存在固有缺陷难以克服。内部管理型规制本质上仍是一种外部监督，无法解决合规动机问题。经过与监管机构的沟通确认，企业制定实施了各类内部管理制度，既有可能出于提升公司绩效考虑，也可能是为了应付检查粉饰门面。企业并非自发遵守合规计划，而是考虑制度成本、外界压力和管理层意见。制度运行成本较低，契合企业盈利模式，得到管理层的支持，内部管理制度可以有效运行；但如果遇到任何一个障碍，内部管理制度运行就可能是“部分的、象征性和半心半意（half-heated）”。〔15〕监管者真正应该关心的是企业管理的实际行动，而不是浮于表面的规章制度，“管理远比管理体系重要”〔16〕。对企业行为的规制，仅仅停留在管理制度上是不够的，需要干预企业管理层或控股股东的合规动机。在这个层面上独立机构的监督职能或许更有意义。

2019 年 7 月美国联邦贸易委员会（FTC）对脸书（Facebook）达成新的和解令，以惩罚脸书违反 2012 年和解令中“禁止虚假陈述”的要求。除了开具 50 亿美元的天价罚单，2019 年和解令还要求脸书改变其董事会构成，设立专门独立隐私委员会。它的所有成员都必须是独立董事，由独立提名委员会产生，每年至少召开 4 次会议。有权任命或免职隐私合规官，每 12 个月审核隐私合规官提交的隐私计划执行情况书面说明。有权任命或免职第三方隐私评估机构，每季度应在没有管理层出席的情况下与其举行会议。每季度审核管理层提交的简报，内容涵盖隐私计划状态、和解令执行情况和存在重大风险情况等等。〔17〕美国联邦贸易委员会的执法意图十分明确，约束限制管理层尤其是控股股东扎克伯格在隐私方面的权力。委员会委员罗希特·乔普拉（Rohit Chopra）发表声明称，脸书通过对外销售用户的行为数据换取广告收入，有强烈的动机获取越来越多的用户数据。只要广告商愿意为用户消费特定内容付费，像脸书这样的公司就有动机以影响用户的心理状态和实时偏好的方式来管理内容。作为一家上市公司，脸书需要与利润丰厚的第三方开发者保持合作，实现公司利益的最大化。〔18〕委员会主席乔·西蒙斯（Joe Simons）和委员诺亚·约书亚·菲利普斯（Noah Joshua Phillips）、克里斯汀·S·威尔逊（Christine S. Wilson）发布声明称，该命令消除了扎克伯格单方面做出隐私决策的能力，赋予业务部门、首席隐私官和隐私委员会相关责任。尽管没有移除扎克伯格对董事会的全部控制权力，但明显地削弱了他的权力，这是迄今为止世界上没有哪个监管机构能做到的。〔19〕

〔15〕 See Christine Parker & Vibeke Lehmann Neelsen, Do Businesses Take Compliance Systems Seriously? An Empirical Study of Implementation of Trade Practices Compliance Systems in Australia, 30 *Melbourne University Law Review* 441 (2006).

〔16〕 前引〔13〕，罗伯特·鲍德温、马丁·凯夫、马丁·洛奇书，第 154 页。

〔17〕 See United States of America v. Facebook Inc, Case No. 19-cv-2184 (United States District Court for the District of Columbia. 2019).

〔18〕 See Rohit Chopra, Dissenting Statement of Commissioner Rohit Chopra, In re Facebook, Inc. Commission File No. 1823109 (July 24, 2019), available at https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf, last visited on Mar. 3, 2022.

〔19〕 See Joe Simons, Noah Joshua Phillips & Christine S. Wilson, Statement of Chairman Joe Simons and Com-missioners Noah Joshua Phillips and Christine S. Wilson In re Facebook, Inc. (July 24, 2019), available at https://www.ftc.gov/system/files/documents/public_statements/1536946/092_3184_facebook_majority_statement_7-24-19.pdf, last visited on Mar. 3, 2022.

通过分析脸书 2012 年和 2019 年两宗案件可知，如果没有触及超大型平台的盈利模式，以及管理层或控股股东对个人信息利用的绝对控制，单纯对超大型平台进行事后监管和流程改造，无法对平台企业的合规动机进行根本影响。因此，需要监督的对象实际是超大型平台的管理层或控股股东。事实上，2012 年和解令最终确定的 4 个月后，脸书就允许第三方开发人员违规使用用户个人信息。〔20〕

由此可见，超大型平台独立机构的制度建构，不仅需要引入政府规制理论，而且应该引入公司治理视角。超大型平台企业的迅速崛起只是近二十年的事情，不少创始人仍然牢牢掌控已经上市的平台企业，并未实现所有权与经营权的分离。脸书的公司结构为 B 级股股东提供了“超级投票权”，扎克伯格的投票决定了董事选举和其他需要股东投票的事项。〔21〕“脸书股东厌倦了扎克伯格，但对他们无能为力。”〔22〕我国存在类似的情况，“作为企业家的发起人或创始股东珍视控制权以实现自己的愿景和抱负，这种对控制权的珍视体现为对发起人或创始股东权利的特殊安排”，如 B 站的双层股权结构、京东的投票委托权和阿里巴巴的合伙人制度等等。〔23〕相较于美国，中国互联网企业模式创新有余而技术创新不足，更加依赖个人信息和人力资源投入。具有类似的公司结构，承担着巨大的利润压力，依靠大量采集个人信息以维持商业运转，我国超级平台管理层或控股股东的合规动力更加匮乏。

四、决策监督型独立机构方案

为加强对管理层或控股股东的控制，不少国家规定董事会负责内控机制建设，赋予董事一定的法律义务。如日本《公司法》规定了董事构建内控机制的任务，《公司法实施规则》规定了构建内控机制的具体内容。〔24〕我国也有学者建议：“想让外部的监督发挥实效，就必须通过内部的决策机构。而内部决策机构最好的做法就是仿效独立董事的相关制度——在董事会下面设立一个主要由独立董事承担监督作用的个人信息保护专门委员会。”〔25〕如果公司董事会全部由管理层组成，那么董事会的存在就没有实际意义，董事会就变成了一个拥有高级头衔的管理委员会了。决策监督型独立机构方案下，我国不少学者建议将外部监督成员理解为公司的独立董事，独立董事组成独立机构负责对企业的个人信息保护作出判断和监督。〔26〕该方案如何展开，具有哪些优势

〔20〕 See FTC Imposes $ 5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, Federal Trade Commission (July. 24, 2019), available at https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions, last visited on Mar. 3, 2022.

〔21〕 参见前引〔18〕，Rohit Chopra 文。

〔22〕 Michael Hiltzik, Facebook Shareholders are Getting Fed Up with Zuckerberg but Can't Do Anything about Him, Los Angeles Times: Business (Apr. 16, 2019), available at https://www.latimes.com/business/hiltzik/la-fi-hiltzik-mark-zuckerberg-facebook-20190416-story.html, last visited on Mar. 13, 2022.

〔23〕 参见汪青松、宋朗：《合规义务进入董事义务体系的公司法路径》，载《北方法学》2021 年第 4 期。

〔24〕 参见梁爽：《内部控制机制的法律化路径——以日本法上董事内部控制义务为视角》，载《金融法苑》2015 年第1 期。

〔25〕 隐私护卫队：《外部机构如何监督企业个人信息保护？许可：不能存在经济依附》，载 https://www.sohu.com/a/509672335_121258695，最后访问时间：2022 年 7 月 23 日。

〔26〕 参见张平主编：《中华人民共和国个人信息保护法理解适用与案例解读》，中国法制出版社 2021 年版，第 225 页；龙卫球主编：《中华人民共和国个人信息保护法释义》，中国法制出版社 2021 年版，第 260 页。

与弊端？现有文献没有对此进行讨论，本文尝试进行探索展开。

（一）方案的理论渊源

该方案与公司治理中的内部控制理论有关。内部控制在会计学和审计学中较为常见，近年来随着法学界对企业合规的关注，逐渐进入法学视野。“内部控制起源于企业财务舞弊、财务失败事件的不断发生，内部控制的发展与美国公司会计造假、破产倒闭事件周期性的发生有着密不可分的关系，每一轮的公司财务舞弊、破产倒闭事件都促进了内部控制理论的发展。”〔27〕例如美国《反海外贿赂法》（FCPA）要求证券发行者必须设计和维持有效的内部会计控制系统。〔28〕我国法律对内部控制理论也有类似应用，例如2021年6月中国人民银行发布的《中华人民共和国反洗钱法（修订草案公开征求意见稿）》第3章“反洗钱义务”第27条第3款规定：“金融机构应当通过内部审计或者独立审计等方式，监督检查反洗钱内部控制制度的有效实施，金融机构的负责人对反洗钱内部控制制度的有效实施负责。”

个人信息保护与企业财务管理存在较大相似性，都涉及企业的不同环节和各个流程，与企业经营模式和利润收支息息相关，关乎企业的生死存亡。尤其在消费者信息隐私意识觉醒的今天，对于超大型平台企业而言，个人信息保护不仅应是其努力控制的成本线，而且应该是严格遵守的生命线。因此，类比财务风险管理，个人信息风险控制完全可以应用内部控制理论。正如学者所说：“内部控制发展到今天，已经演变成一种过程，内化于企业的各个流程、各个环节，和企业的各类人员相联系，但从内部控制的对象和目标来看，其本质并没有发生变化，依然是一种风险控制活动。”〔29〕内部控制与风险管理属于一体两面，本质上都是对风险的有意控制。“内部控制就是控制风险，控制风险就是风险管理。”“内部控制主要是从风险控制的方式和手段说明风险控制的，风险管理就是从风险控制的目的来说明风险控制的。”〔30〕为强调对管理层和控股股东的力量制衡，避免风险管理和企业管理概念混淆，本文采用内部控制的概念。

对于内部控制的定义，美国国家金融欺诈信息委员会（Treadway委员会）下属的“发起组织委员会”（COSO）〔31〕发布的《COSO内部控制—综合框架（2013）》指出，内部控制是一个由实体董事会、管理层和其他人员实施的过程，旨在为实现运营、报告和合规相关目标提供合理保证。合规目标与遵守实体法律法规有关。这一框架包含控制环境、风险评估、控制活动、信息交流和监控活动五个组成部分。〔32〕我国财政部、证监会、银监会等五部委于2008年5月发布的《企业内部控制基本规范》第3条规定：“本规范所称内部控制，是由企业董事会、监事会、经理

〔27〕 李维安、戴文涛：《公司治理、内部控制、风险管理的关系框架——基于战略管理视角》，载《审计与经济研究》2013年第4期，第5页。

〔28〕 See The Foreign Corrupt Practices Act of 1977 § 15 U. S. C. § 78dd-1, et seq.

〔29〕 前引〔27〕，李维安、戴文涛文，第6页。

〔30〕 谢志华：《内部控制、公司治理、风险管理：关系与整合》，载《会计研究》2007年第10期，第41页。

〔31〕 COSO英文全称为Committee of Sponsoring Organizations of the Treadway Commission。COSO在美国成立于1985年，旨在赞助国家金融欺诈信息委员会（Treadway委员会）。Treadway委员会最初由位于美国的以下五家主要专业会计协会和机构发起和共同资助：美国注册会计师协会（AICPA）、美国会计协会（AAA）、国际财务执行官（FEI）、内部协会审计师（IIA）和管理会计师协会（IMA）。

〔32〕 See The Committee of Sponsoring Organizations of the Treadway Commission（COSO），COSO Internal Control-Integrated Framework（2013）（May 14，2013），available at https://assets.kpmg/content/dam/kpmg/pdf/2016/05/2750-New-COSO-2013-Framework-WHITEPAPER-V4.pdf，last visited on Feb. 13，2022.

层和全体员工实施的、旨在实现控制目标的过程。内部控制的目标是合理保证企业经营管理合法合规、资产安全、财务报告及相关信息真实完整，提高经营效率和效果，促进企业实现发展战略。”企业控制目标的实现需要由股东会、董事会、监事会和管理层等各个组织机构共同完成。构建合规制度体系是内部控制目标，无论由董事会或监事会设置独立机构，它们开展的内部监督活动都属于风险控制的内部过程。

该理论强调应发挥董事会内部控制的主导作用，例如《上海证券交易所上市公司内部控制指引》第 4 条规定：“公司董事会对公司内控制度的建立健全、有效实施及其检查监督负责，董事会及其全体成员应保证内部控制相关信息披露内容的真实、准确、完整。”比较法上，韩国存在类似的“合规监查人”制度。“合规监查人通常从公司内部的董事或业务执行负责人中选任，其虽由董事会任命，但却独立履行职务，其业务活动不受董事会或代表董事的干预。为了保障其独立性地位，韩国《金融公司治理结构法》第 30 条要求金融公司应当通过章程保障合规监查人独立履行职务，并为其履行职务提供必要的资料和信息；对合规监视人的任免虽由公司自主决定，但须在作出决定之日起 7 天内向金融委员会报告。公司未按规定设置合规监视人或未按照合规要求进行报批和运营的，根据该法第 43 条第 16—22 款的规定，可对其处以罚款。”〔33〕

美国学者提出了应由董事会承担内部控制最终责任的两点理由：第一，企业高管有可能扭曲信息流动。解决信息不对称问题，创造竞争性的信息来源。第二，存在管理机会主义问题。管理层面临业绩压力，任期薪酬与企业盈利高度相关。在一笔违反公司政策或法律规则的交易中，预期的利润通常是巨大、现实和生动的。相比之下，从经理的角度来看，违反公司政策或法律规则可能造成的损失往往微不足道、苍白、非常遥远，尤其是考虑到发现的可能性极低时，情况更是如此。董事们不寻求晋升，通常不负责短期利润决策判断，因而对于公司整体和长远利益更加看重。〔34〕脸书案件体现了该学者的公司治理思路，2019 年和解令创造了加强脸书隐私监管的四个信息流，建构了一种重叠的合规监督渠道（overlapping channels of compliance），以提高风险防控效率。〔35〕为加强对某一重要事项的整体管理，董事会设置专门委员会的做法在实践中已经很常见。如很多上市公司在董事会设立社会责任专门委员会和环境保护专门委员会。〔36〕

（二）设在董事会下而不是监事会下

内部控制职责的权能配置，实际上与不同国家公司法规定的组织结构有关。“英美法国家实行的主要是以外部董事为核心的监督制度，它与我国的独立董事制度相似。在以德国为代表的大陆法国家，实行的主要是以监事会为核心的监督制度。”〔37〕我国《公司法》规定董事会和监事会两个组织机构负责内部监督职能。有的学者认为转换到中国背景下监事同样负有内部控制义务。〔38〕我国《公司法》虽然没有明确规定外部监事制度，但是部分企业早已开始探索实施，如

〔33〕 赵万一：《合规制度的公司法设计及其实现路径》，载《中国法学》2020 年第 2 期，第 76 页。

〔34〕 See Melvin A. Eisenberg, The Board of Directors and Internal Control, 19 *Cardozo Law Review* 237, 250 (1997).

〔35〕 参见前引〔19〕，Joe Simons、Noah Joshua Phillips、Christine S. Wilson 文。

〔36〕 参见蒋大兴：《公司社会责任如何成为“有牙的老虎”——董事会社会责任委员会之设计》，载《清华法学》2009 年第 4 期。

〔37〕 高旭军：《对我国上市公司“双核心监督机制”的反思》，载《东方法学》2016 年第 2 期，第 58 页。

〔38〕 参见邢会强：《上市公司虚假陈述行政处罚内部责任人认定逻辑之改进》，载《中国法学》2022 年第 1 期。

中国人民银行2002年就曾发布《股份制商业银行独立董事和外部监事制度指引》。有学者提出独立董事的监督是决策中的监督，监事会的监督体现为事后监督。〔39〕以上观点和实践都具有借鉴意义，存在两个内部监督机关的情况下，董事会和监事会都可以承担个人信息保护的内部控制职责。需要进一步思考的是，为落地实施《个人信息保护法》，是否需要《公司法》相应修改，董事会和监事会哪一个组织更具有设置独立机构的制度潜力。

本文认为在坚持现有公司法框架下，独立机构更适合设置在董事会中，主要成员由独立董事担任。为了解决监事会存在的问题，我国引入了独立董事制度。公司监事会作为专门监督机构，普遍存在“监事会地位低下、资源匮乏，职工监事制度徒具其形，监事缺乏适当的考核和激励机制，与独立董事关系不清、叠床架屋，受制于高管控股股东”等问题。〔40〕不同学者总结的原因或有出入，但是监事会孱弱无力确是现实，无力对抗控股股东实施有效监督。我国《公司法》规定监事会由股东代表和职工代表组成，职工代表的比例不得低于三分之一，意图加强股东和雇员对公司的自我监督。但股东代表产生受制于控股股东，职工代表履职遭雇佣关系掣肘。即便允许外部监事加入，也难以改变监事会的固有缺陷。独立机构要求主要由外部成员组成，这与监事会的人员比例要求也存在出入。董事会拥有解聘或聘任管理层和制定规章制度等事项的决定权，可以有效建构个人信息保护内控合规体系。但是监事会仅具有建议、质询和调查等权利，只能列席董事会会议，没有投票表决权和否决权。我国超大型平台企业多赴美股和港股上市，就个人信息保护问题对董事会进行改造，与英美公司法传统不存在较大差异，更有利于企业降低合规成本。

（三）独立董事需要平衡股东利益与公共利益

独立机构由独立董事构成，独立董事实际开展监督活动，但是独立董事应该对谁负责，却鲜有学者深入研究。有专家观察到存在利益冲突的可能，有针对性地提出“如果认为独立监督机构对社会公众负责，公司的发展利益或将不作为独立监督机构考虑的范畴，有可能导致公司发展利益受损”〔41〕。这些观察实际上点出了问题的实质，独立董事应该对公共利益负责，还是对企业利益和股东利益负责？《上市公司独立董事规则》第5条规定独立董事应该维护公司整体利益，尤其要关注中小股东的合法权益不受损害。但是超大型平台收集了大量的公民个人信息，即便个人信息处理者投入了汗水劳动，个人信息蕴含的人格利益仍然属于公民或用户个人。空泛地说，公司利益、股东利益与社会公共利益当然是一致的，企业违反法律规定侵犯公共利益受到法律制裁，也会损害企业利益和股东利益。“但这个观点其实只是体现了一种‘大家好才是真的好’的良善价值导向，在逻辑上就如同个体利益和群体利益可以两全的论断一样脆弱，如果真的可以两全就不会有损公肥私和牺牲小我完成大我的问题。”〔42〕事实上滥用公民个人信息的现象已经如此普遍，大量的违法行为并没有被发现惩处，有些人甚至怀疑是否还有继续保护的必要。因此，实践中公司利益、股东利益与公共利益广泛存在着利益冲突。努力追求私人利益，既有可能成为创

〔39〕 参见施天涛：《让监事会的腰杆硬起来——关于强化我国监事会制度功能的随想》，载《中国法律评论》2020年第3期。

〔40〕 参见郭雳：《中国式监事会：安于何处，去向何方？》，载《比较法研究》2016年第2期。

〔41〕 虞伟：《个保法要求建外部独立监督机构，互联网平台为何按兵不动》，载 https://xw.qq.com/cmsid/20211111A009I900，最后访问时间：2022年7月23日。

〔42〕 前引〔23〕，汪青松、宋朗文，第81页。

新创业的动力源泉，也有可能是公地悲剧的罪魁祸首。盲目乐观与有意回避都不可取，在流通利用中个人信息才能发挥实际价值。真正值得思考的是，如何通过法律规则调整实现不同利益平衡。

传统公司法理论认为董事仅对股东利益负责，追求股东利益最大化。基于公司所有权与经营权分离的现实情况，股东选举产生董事负责实际经营，股东与董事之间属于委托代理关系，董事对股东负有信义义务，通说认为至少包含忠实义务和勤勉义务。尽管从 19 世纪 30 年代开始，美国学界开启的企业社会责任讨论一直延续至今，但是这一框架仍是公司法的基本理论模型。正如前美国特拉华州最高法院首席大法官小利奥·E·斯特林（Leo E. Strine，Jr.）所说，“这些公司的董事会认为，他们所管理的共和国应该对唯一公民忠诚，而这些公民被称为股东。这些公司的董事会并不认为自己对其他选区有任何国家的忠诚度，他们认为自己是股权资本共和国的民选官员。”〔43〕但是董事追求股东利益并非没有限度，必须遵守法律的各项要求，意味着对于法律强制性规定事项，董事不能进行成本收益比较，这实际上在法律框架内限制了股东利益。伴随着美国公司所有权与经营权的分离，众多学者提出应该考虑企业的社会责任，公司董事会不仅要对股东利益负责，而且要考虑消费者、社区、雇员、客户和环境保护等非股东利益，由此产生了诸如利益相关者理论、公司公民理论、公司善治运动等理论思潮。〔44〕公司生产经营会产生各种社会成本，污染环境、劳工、金融风险等问题都需要公司经营者认真考虑。立法者希望通过成文立法解决这些问题，规定企业相应的法律义务，我国《个人信息保护法》也是如此。企业毕竟不是政府，企业存在的根本目的仍是追逐利润。曾经有人建议在公司董事会设立代表不同群体利益的公益董事，有学者评论说，即便全部董事追求公司利益最大化，都不一定可以实现意见统一。如果董事会充斥着目标不同相互竞争的支持者，那将是大多数管理者的噩梦。〔45〕如果赋予企业过多的公共责任，可能会将企业经营变成政治活动，董事之间的实质性利益冲突会导致公司无法经营。由此可知，如同公司一样，董事会既不可能彻底坚持“股东至上”，也无法完全替代政府追求公共利益，坚持维护股东利益兼带平衡公共利益才是现实选择。在个人信息保护问题上同样如此，个人信息只有在聚合、加工和利用之后才能发挥最大价值，平台企业的产品创新和商业开发在其中发挥了不可替代的作用，规范利用是最终目的，违规惩戒只是手段。因此，独立机构作为董事会的下设机构，需要平衡股东利益和公共利益。部分学者认为它不对个人信息处理者负责、单纯维护公共利益、应该保持中立性的观点是错误的。

独立董事作为独立机构的成员，应追求实现企业利益，我国《公司法》第 147 条和《上市公司独立董事规则》第 5 条均有直接规定。与《公司法》立法目的不同，《个人信息保护法》不要求独立董事关注中小股东的合法权益，而是强调他们对个人信息保护情况进行有效监督，主要关注广大力量分散的公民个人信息权益，本质上属于一种利益相关者权益。这部分利益与中小股东利益风险偏好存在明显不同，但是它们都依附在公司整体利益之上。无论是维护中小股东利益，

〔43〕 Leo E. Strine Jr.，Corporate Power is Corporate Purpose II：An Encouragement for Future Consideration from Professors Johnson and Millon，74 *Washington and Lee Law Review* 1，13（2017）.

〔44〕 参见施天涛：《〈公司法〉第 5 条的理想与现实：公司社会责任何以实施?》，载《清华法学》2019 年第 5 期。

〔45〕 See Alfred F. Conard，Reflections on Public Interest Directors，75 *Michigan Law Review* 941，950（1977）.

还是为了公民个人信息权益，法律为分散的利益群体选派代表，都试图打破控股股东的非对称权利结构，努力干预影响公司决策。二者在规制思路上是相似的，这是嫁接独立机构职能与独立董事职责的基础。股东利益、公司利益和公共利益，三者在合规层面是一致的。法律底线不容利益权衡，遵纪守法保障企业长远。这解释了为什么设置独立机构是构建合规体系的一部分，为什么独立机构与合规体系共同组成《个人信息保护法》第58条第1项。

（四）独立董事承担的法律义务之性质

结合我国《公司法》，独立董事的这种内部控制行为属于什么法律义务？我国《公司法》第147条规定董事对公司负有忠实和勤勉义务，《上市公司独立董事规则》第5条规定独立董事对上市公司及全体股东负有诚信与勤勉义务。这里出现了三种义务类型：忠实义务、诚信义务和勤勉义务，内部控制与三者是什么关系？法律义务这一概念本质要求主体行为符合法律规定，文字意义上所有部门法规定的各项法律义务都属于“合规义务”，但是某一种“合规行为”能否成为独立具体的法律义务就值得讨论了。这些新增的合规义务是否属于信义义务？或者它们可以成为一种新的“合规义务”？存在独立的内部控制义务吗？目前主要存在三种观点：第一，内部控制行为属于忠实义务或诚信义务的一种。诚信义务是否属于一种单独的信义义务类型，在美国公司法上存在着“三分法”和“二分法”的争议。本文无意对此进行明确区分，故将忠实义务与诚信义务进行并列。有学者提出，美国法上在董事违反内部控制机制建构义务的案例中，如Caremark案以及Stone案，法院一般认为董事故意忽视自身职责，往往会判定董事违反忠实义务。〔46〕第二，内部控制行为属于勤勉义务或注意义务的一种。有学者提出：“就履行个人信息保护法定义务而言，在学理上属于公司董事、高管应当履行的勤勉义务，即公司管理者应当保障公司能够切实履行法律规定的保护个人信息的义务，从而维护公司的利益，避免公司因义务不履行而遭受不利的法律后果，诸如，损害赔偿、行政处罚，甚至刑事处罚。”〔47〕有学者认为内部控制义务是董事勤勉义务的具体化和内在化，认为“对企业发生的重大事件或事故，即使是无需董事亲自决策和具体实施的小事直接引起的，如果该重大事件或事故与内部控制的不健全有关联，是和未能建立健全能尽早发现纠正违法违规事件的源头原因，防止事件发生的公司内部控制有关联，在一定条件下，也应认定董事违反了内部控制义务，董事应对公司承担相应的损害赔偿责任”〔48〕。还有学者分析德国公司法，论证从业务执行机构的谨慎义务中引申出来的合法性管控义务可以成为合规组织义务的法律基础。〔49〕第三，内部控制属于一种特殊的合规义务，与董事信义义务并列。有学者认为“董事信义义务的产生原因系董事与公司及股东间的委托代理关系和利益冲突，旨在减少公司治理中的代理成本。而董事的合规义务源于公司行为的合法性要求从组织层面向个体层面的下沉，旨在减少公司经营中的社会成本”，两种法律义务的产生原因存在根本不同，因此势

〔46〕 参见梁爽：《董事信义义务结构重组及对中国模式的反思——以美、日商业判断规则的运用为借鉴》，载《中外法学》2016年第1期。

〔47〕 张怀岭：《公司治理视域下个人信息保护的实现路径——以〈公司法〉第147条的具体化为中心》，载《财经法学》2018年第5期，第28页。

〔48〕 刘惠明、祁靖：《内部控制义务——董事勤勉义务的具体化与内在化》，载《东南大学学报（哲学社会科学版）》2012年第5期，第76页。

〔49〕 参见王东光：《组织法视角下的公司合规：理论基础与制度阐释》，载《法治研究》2021年第6期。

必产生张力与冲突。〔50〕

客观分析上述观点学说都有其合理之处，内部控制并非一个法学概念，包括公司治理、风险管理和企业合规的各个流程，这决定了其行为本身可能属于广义信义义务其中的一种类型，需要将《个人信息保护法》第 58 条和信义义务的子义务做综合理解，利用忠实义务、诚信义务和勤勉义务拓展个人信息保护义务的实质内容。应该避免法律义务的“大词化”倾向，尽量提供一些充满血肉的制度安排。《公司法》修订过程中，部分学者建议将合规义务确立为公司和相关成员的基本义务，借此建构整个合规理论体系。〔51〕但是加入合规义务可能导致本就抽象的信义义务更加混乱，增加无谓的概念重叠与指向冲突。因此，本文不建议将内部控制行为作为一种新型合规义务，借由合规义务与信义义务并列的方式在《公司法》上确立下来。正如学者所说：“一个连注意义务都没有能力去具体界定的法律制度，如何去设定在此基础上更复杂的合规?”〔52〕

（五）职能设计和人员构成

在职能设计上，独立机构的监督职能体现为两方面：第一，监督职能本质上是督导并举而非狭义监督，应该扩充独立机构的实际职能。不同于外部监督事后纠错，独立机构的监督活动是对个人信息风险的内部控制活动，不仅局限于监控活动，而且包括控制环境、风险评估、控制活动、信息交流四个环节。第二，监督职能属于系统监督而非具体监督，应该减轻独立机构的职责负担。超大型平台企业规模巨大，包含各种业务类型，难以指望任职董事进行具体监督。“董事负有对公司作为一个运行良好的系统的‘设计者’和‘维护者’的职责，负有督导（monitor）的义务。”〔53〕系统监督与具体监督的不同，是划分独立机构与个人信息保护负责人工作职责的重要标准。

在人员构成上，专门委员会人员数量应保持单数，由三名或三名以上成员组成。可根据实际情况，由董事会提名委员会动态调整。独立董事应至少占全部人员三分之二及以上。其余三分之一，控股股东和负责个人信息保护的高级管理人员不得担任。为不干扰企业正常经营，在日常性管理中独立董事由超大型平台企业自行选任，平台企业应及时向主管部门备案公示。在合规整改时，为保证整改措施及时到位，可由主管部门指定独立董事人选。独立董事的任职条件，除了符合《上市公司独立董事规则》的各项要求外，还应该强调专业性与多样性。鼓励企业聘请具有一定个人信息保护专业知识的法律、计算机、企业管理等领域专家进入专门委员会。考虑到承担系统监督的工作职责，专门委员会成员理应从平台企业领取适当报酬。

（六）方案存在的弊端

决策监督型独立机构方案将独立机构设置在董事会内部，由独立董事具体履行监督职责，独立于董事经理等高级管理人员，具有一定的合理之处。同时也存在诸多弊端：第一，各种独立董事组成的专业委员会过多，容易造成董事会负担过重。机构人员臃肿效率低下。环境保护委员会、合规委员会、劳工权益委员会、可持续发展委员会、社会责任专门委员会等各种委员会都多

〔50〕 参见前引〔23〕，汪青松、宋朗文。

〔51〕 参见前引〔33〕，赵万一文。

〔52〕 邓峰：《公司合规的源流及中国的制度局限》，载《比较法研究》2020 年第 1 期，第 44 页。

〔53〕 邓峰：《领导责任的法律分析——基于董事注意义务的视角》，载《中国社会科学》2006 年第 3 期，第 143－144 页。

少已经存在，有些是法律强制规定的，有些是企业根据自身情况设立的，不同委员会之间存在职能重叠，很容易造成独立董事身兼多职负担过重。第二，独立董事平衡股东利益、利益相关者利益和公共利益，虽然理论上可以抽象证成，但实际操作存在困难。加之独立董事职能责任众多，很难周全各种利益诉求。第三，独立董事法律责任不明，容易挫伤独立董事的积极性。2021 年 11 月 12 日广州市中级人民法院判决康美药业五名独立董事因违反勤勉义务承担连带责任，合计赔偿金额最高约 3.69 亿元。此案引发了有关独立董事法律责任的争论。我国独立董事多为兼职担任，无论是信息来源、时间精力，还是对企业业务的了解程度，实际上都无法与公司董监高相比，在客观条件受限的情况下倡导提高独立董事法律责任存在一定问题。我国《公司法》欠缺对勤勉或注意义务的制度化建构，二者本身是一个不确定法律概念，内涵外延都有待明确。《个人信息保护法》虽然已颁布实施，但是为时尚短仍需实践，不少具体规则也仍在探索之中，极有可能造成权责畸轻畸重。

五、结语：合规监督的模式选择

根据上文分析可知，第三方独立机构方案欠缺独立性，不具有比较优势，无法承载《个人信息保护法》第 58 条第 1 项的功能期待，因此该方案应该被否定舍弃。管理监督型独立机构方案可以实现对经理层和业务部门的日常监督，但无法解决独立机构对谁负责的问题，由于难以介入董事会决策，始终面临企业合规动力不足的问题。决策监督型独立机构方案，虽然实现了对企业管理层的全面监督，但是容易发生利益冲突，日常情况下难以区分不同利益诉求，受制于法律义务规定模糊，容易承担过重的法律责任。由此可见，无论是管理监督型独立机构方案，还是决策监督型独立机构方案，都存在合理之处与固有弊端。能否通过制度安排扬长避短呢？超大型平台侵犯个人信息具有隐蔽性，宏观决策、中观执行和微观操作都需要进行有效合规和必要监督。两种监督方案都属于合规监督的具体类型，只能在各自的制度场景下合理运行，无法通过一种模式解决所有问题，需要明确两种方案所属的合规监督模式。

根据已有文献研究，管理监督型独立机构方案应属于“日常性合规管理模式”的具体展开，该模式是指“企业在没有违法、违规或者犯罪的情况下，根据常态化的合规风险评估结果，为防范企业潜在的合规风险，开展合规管理体系建设”〔54〕。这种合规监督模式关注日常管理和风险预防，独立机构主要监督业务部门实际运作和搭建完整合规体系，在企业没有出现重大安全风险和受到法律制裁时，只需对董事会负责即可，显然无需任何决定和认定都向主管部门报告。决策监督型独立机构方案应属于“危机性合规整改模式”，该模式是指“企业在面临行政执法调查、刑事追诉或者国际组织制裁的情况下，针对自身在经营模式、管理方式、决策机制等方面存在的漏洞和隐患，进行有针对性的制度修复和错误纠正”〔55〕。在此种模式下，该方案的问题可迎刃而解。为指导涉事企业有针对性进行合规整改，执法机构可选派政府工作人员或法律专家担任企业

〔54〕 陈瑞华：《有效合规管理的两种模式》，载《法制与社会发展》2022 年第 2 期，第 6 页。

〔55〕 前引〔54〕，陈瑞华文，第 6 页。

独立董事，此时仍处于危机应对阶段，因此各方利益诉求相对清晰，实现企业合规和恢复正常经营是多方主体的最大利益公约数。根据执法机构出具的合规整改意见，独立董事的监督义务明确，由此承担不合比例法律责任的情形很难出现。同时，独立机构的监督对象是整个企业管理层，外部监督直接介入企业运行，此时独立董事向主管部门汇报整改情况，在法律上也并不存在解释障碍。综上所述，管理监督型独立机构方案适用于日常性合规管理模式，决策监督型独立机构方案适用于危机性合规整改模式。在区分日常管理和危机应对两种合规监督场景下，两种方案的制度优势可以最大程度发挥，而制度劣势可以相对减弱。

Abstract: Paragraph 1 of Article 58 of the Personal Information Protection Law stipulates that super large platform enterprises should establish independent institutions mainly composed of external members to supervise the protection of personal information. At present, there are three system design schemes. The third-party independent institution scheme has no obvious comparative advantages, does not conform to the concept of risk prevention, and is difficult to carry the expectation of supervision function, so it should be abandoned. The plan of management and supervision independent institution belongs to the daily compliance management mode, which is the management supervision of the board of directors to the managers. The activities of independent institutions under the leadership of the board of directors can not solve the problem of compliance motivation, and it is difficult to clarify the tension between the board of directors and law enforcement agencies. The decision-making supervision type independent institution scheme belongs to the crisis compliance rectification mode, which is the rectification supervision of the law enforcement agency to the board of directors. A special committee of the board of directors is established to rely on independent directors for internal control. However, the legal responsibilities of independent directors are vague, which is easy to cause overburden on the board of directors. The two schemes have their own advantages and disadvantages, and should be applied separately according to the problem scenarios to realize the systematic and continuous protection of citizens' personal information.

Key Words: super large platform, independent institution, management supervision, decision supervision

（责任编辑：周　游　赵建蕊）